take a look

SECOND CLASS POSTAGE
Permit PAID at
East Setauket, N.Y.
11733
ISSN 0749-3851

2600 Magazine
PO Box 752
Middle Island, NY 11953 U.S.A.
Forwarding and Address Correction Requested

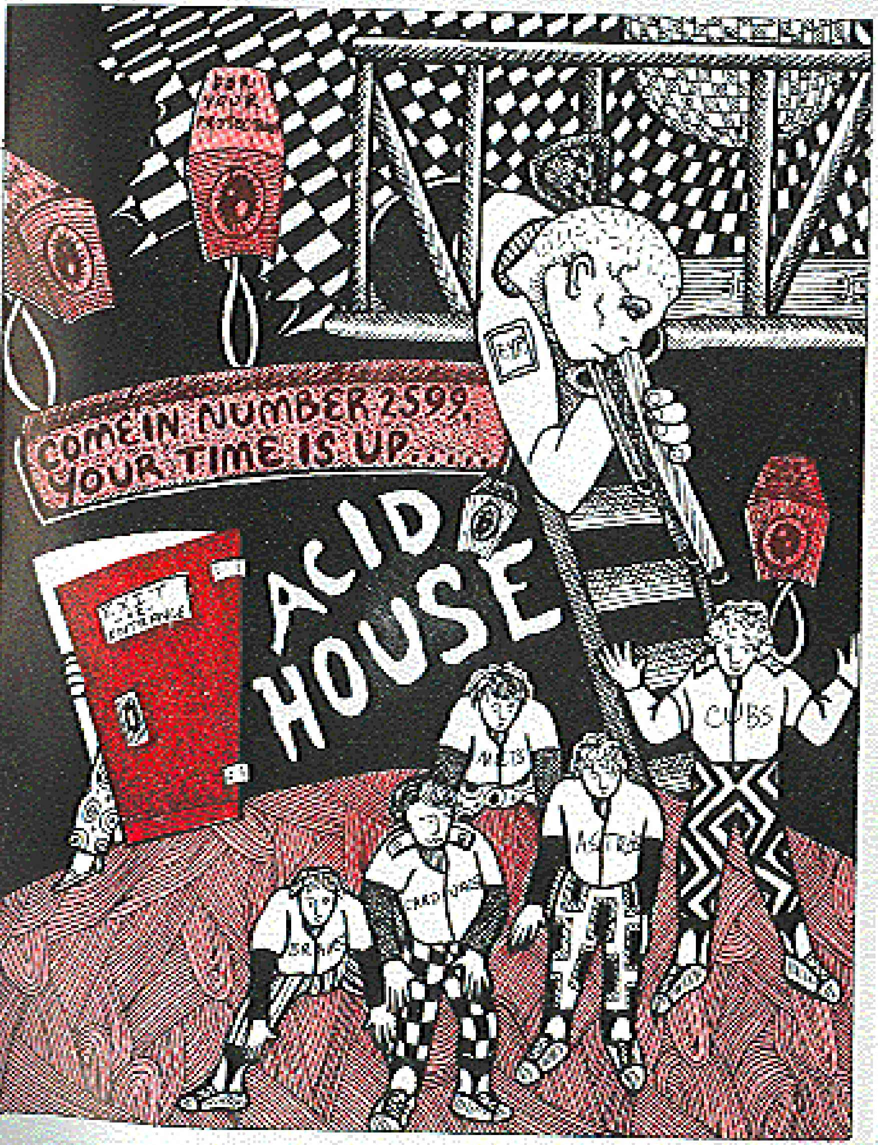
LOD^3 . [illegible]

2600

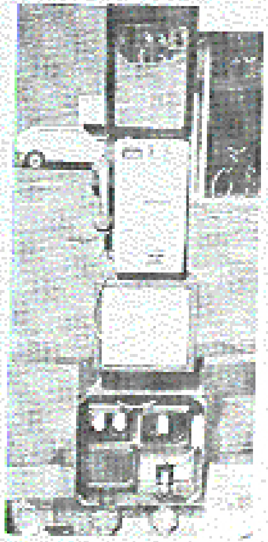
The Whole World's Watching

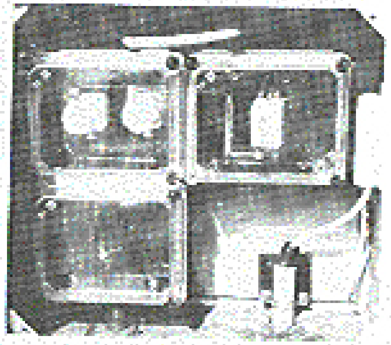
The Hacker Quarterly

VOLUME SEVEN, NUMBER ONE!
SPRING, 1990



NAKED DUTCH PAYPHONES
In the streets of Amsterdam





AND A FULLY CLOTHED ONE
In Australia

SEND YOUR PAYPHONE PHOTOS TO: 2600 PAYPHONES, PO BOX 99, MIDDLE ISLAND, NY 11953.

2600 (ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc., 7 Strong's Lane, Setauket, NY 11733. Second class postage permit paid at Setauket, New York.
POSTMASTER: Send address changes to
2600, P.O. Box 752, Middle Island, NY 11953-0752.

Yearly subscription: U.S. and Canada -- $18 individual, $45 corporate.
Overseas -- $30 individual, $65 corporate.
Back issues available for 1984, 1985, 1986, 1987, 1988, 1989
at $25 per year, $30 per year overseas.

ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:
2600 Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752.
FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099.
NETWORK ADDRESSES: 2600@well.sf.ca.us, 2600@dasys1.UUCP.

***2600* Office Line: 516-751-2600, *2600* FAX Line: 516-751-2608**

FOR YOUR PROTECTION

A year ago, we told the stories of Kevin Mitnick and Herbert Zinn, two hackers who had been sent to prison. It was then, and still is today, a very disturbing chain of events: mischief makers and explorers imprisoned for playing with the wrong toys and for asking too many questions. We said at the time that it was important for all hackers to stand up to such gross injustices. After all, they couldn't lock us all up.

It now appears that such an endeavor may indeed be on the agendas of some very powerful U.S. governmental agencies. And even more frightening is the realization that these agencies don't particularly care who or what gets swept up along with the hackers, as long as all of the hackers get swept up. Apparently, we're considered even more of a threat than we had previously supposed.

In retrospect, this doesn't come as a great deal of a surprise. In fact, it now seems to make all too much sense. You no longer have to be paranoid or of a particular political mindset to point to the many parallels that we've all been witnesses to. Censorship, clampdowns, "voluntary" urine tests, lie detectors, handwriting analysis, surveillance cameras, exaggerated crises that invariably lead to curtailed freedoms.... All of this together with the overall view that if you're innocent, you've got nothing to hide. And all made so much more effective through the magic of high tech. Who would you target as the biggest potential roadblock if not the people who *understand* the technology at work? It appears the biggest threats to the system are those capable of manipulating it.

What we're about to tell you is frightening, plain and simple. You don't have to be a hacker to understand this. The words and ideas are easily translatable to any time and any culture.

Crackdown

"We can now expect a crackdown....I just hope that I can pull through this one and that my friends can also. This is the time to watch yourself. No matter what you are into.... Apparently the government has seen the last straw in their point of view.... I think they are going after all the 'teachers'...and so that is where their ener-

FOR YOUR OWN GOOD

gies will be put to stop *all* hackers, and stop people *before* they can become threats."

This was one of the reactions on a computer bulletin board to a series of raids on hackers, raids that had started in 1989 and spread rapidly into early 1990. Atlanta, St. Louis, and New York were major targets in what was then an undetermined investigation.

This in itself wouldn't have been especially alarming, since raids on hackers can almost be defined as commonplace. But this one was different. For the very first time, a hacker newsletter had also been shut down.

Phrack was an electronic newsletter published out of St. Louis and distributed worldwide. It dealt with hacker and phone phreak matters and could be found on nearly all hacker bulletin boards. While dealing with sensitive material, the editors were very careful not to publish anything illegal (credit card numbers, passwords, Sprint codes, etc.). We described "Phrack World News" (a regular column of *Phrack*) in our Summer 1989 edition as "a must-read for many hackers". In many ways *Phrack* resembled *2600*, with the exception of being sent via electronic mail instead of U.S. Mail. That distinction would prove to be *Phrack*'s undoing.

"Apparently, we're considered even more of a threat than we had previously supposed."

It now turns out that all incoming and outgoing electronic mail used by *Phrack* was being monitored by the authorities. Every piece of mail going in and every piece of mail coming out. These were not pirated mailboxes that were being used by a couple of hackers. These had been obtained legally through the school the two *Phrack* editors were attending. Privacy on such mailboxes, though not guaranteed, could always be assumed. Never again.

It's fairly obvious that none of this would have happened, none of this *could* have happened had *Phrack* been a non-electronic magazine. A printed magazine would not be intimidated into giving up its mailing list as *Phrack* was. Had a printed magazine been shut down in this fashion after having all of their mail opened and read, even the most thick-headed sensationalist media types would have caught on: hey, isn't that a violation of the First Amendment?

Those media people who understood what was happening and saw the implications were very quickly drowned out in the hysteria that followed. Indictments were being handed out. Publisher/editor Craig Neidorf, known in the hacker world as Knight Lightning, was hit with a seven count indictment accusing him of participating in a scheme to steal information about the enhanced 911 system run by Bell South. Quickly, headlines screamed that hackers had broken into the 911 system and were interfering with emergency telephone calls to the police. One newspaper report said there were no indications that anyone had died or been injured as a result of the intrusions. What a relief. Too bad it wasn't true.

In actuality there have been very grievous injuries suffered as a result of these intrusions. The intrusions we're referring to are those of the government and the media. The injuries have been suffered by the defendants who will have great difficulty resuming normal lives even if all of this is forgotten tomorrow.

And if it's not forgotten, Craig Neidorf could go to jail for more than 30 years and be fined $122,000. And for what? Let's look at the indictment:

"It was... part of the scheme that defendant Neidorf, utilizing a computer at the University of Missouri in Columbia, Missouri would and did receive a copy of the stolen E911 text file from defendant [Robert J.] Riggs [located in Atlanta and known in the hacker world as Prophet] through the Lockport [Illinois] computer bulletin board system through the use of an interstate computer data network.

"It was further part of the scheme that defendant Neidorf would and did edit and retype the E911 Practice text file at the request of the defendant Riggs in order to conceal the source of the E911 Practice text file and to prepare it for publication in a computer hacker newsletter.

"It was further part of the scheme that defendant Neidorf would and did transfer the stolen E911 Practice text file through the use of an interstate computer bulletin board system used by defendant Riggs in Lockport, Illinois.

"It was further part of the scheme that the defendants Riggs and Neidorf would publish information to other computer hackers which could be used to gain unauthorized access to emergency 911 computer systems in the United States and thereby disrupt or halt 911 service in portions of the United States."

Basically, Neidorf is being charged with *receiving* a stolen document. There is nothing anywhere in the indictment that even suggests he entered any computer illegally. So his crimes are receiving, editing, and transmitting.

Now what is contained in this document? Information about how to gain unauthorized access to, disrupt, or halt 911 service? Hardly. The document (erroneously referred to as "911 software" by the media which caused all kinds of misunderstandings) is quoted in *Phrack* Volume 2, Number 24 and makes for one of the dullest articles ever to appear in the newsletter. According to the indictment, the value of this 20k document is $79,449. **[See related story, page 37]**

Shortly after the indictments were handed down, a member of the Legion of Doom known as Erik Bloodaxe issued a public statement. "[A group of three hackers] ended up pulling files off [a Southern Bell system] for them to look at. This is usually standard procedure: you get on a system, look around for interesting text, buffer it, and maybe print it out for posterity. No member of LOD has ever (to my knowledge) broken into another system and used any information gained from it for personal gain of any kind...with the exception of maybe a big boost in his reputation around the underground. [A hacker] took the documentation to the system and wrote a file about it. There are actually two files, one is an overview, the other is a glossary. The information is hardly something anyone could possibly gain anything from except knowledge about how a certain aspect of the telephone company works."

"They are going after all the 'teachers'."

He went on to say that Neidorf would have had no way of knowing whether or not the file contained proprietary information.

Prosecutors refused to say how hackers could benefit from the information, nor would they cite a motive or reveal any actual damage. In addition, it's widely speculated that much of this information is readily available as reference material.

In all of the indictments, the Legion of Doom is defined as *"a closely knit group of computer hackers involved in: a) disrupting telecommunications by entering computerized telephone switches and changing the routing on the circuits of the computerized switches; b) stealing proprietary computer source code and information from companies and individuals that owned the code and information; c)*

FOR YOUR PROTECTION

stealing and modifying credit information on individuals maintained in credit bureau computers; d) fraudulently obtaining money and property from companies by altering the computerized information used by the companies; e) disseminating information with respect to their methods of attacking computers to other computer hackers in an effort to avoid the focus of law enforcement agencies and telecommunication security experts."

Ironically, since the Legion of Doom *isn't* a closely knit group, it's unlikely that anyone will be able to defend the group's name against these charges — any defendants will naturally be preoccupied with their own defenses. (Incidentally, Neidorf was not a part of the Legion of Doom, nor was *Phrack* a publication of LOD, as has been reported.)

The Hunt Intensifies

After learning of the *Phrack* electronic mail surveillance, one of the system operators of *The Phoenix Project*, a computer bulletin board in Austin, Texas, decided to take action to protect the privacy of his users. "I will be adding a secure encryption routine into the e-mail in the next 2 weeks - I haven't decided exactly how to implement it, but it'll let two people exchange mail encrypted by a password only known to the two of them.... Anyway, I do not think I am due to be busted...I don't do anything but run a board. Still, there is that possibility. I assume that my lines are all tapped until proven otherwise. There is some question to the wisdom of leaving the board up at all, but I have personally phoned several government investigators and invited them to join us here on the board. If I begin to feel that the board is putting me in any kind of danger, I'll pull it down with no notice - I hope everyone understands. It looks like it's sweeps-time again for the feds. Let's hope all of us are still around in 6 months to talk about it."

> *"All incoming and outgoing electronic mail used by Phrack was being monitored by the authorities."*

The new security was never implemented. *The Phoenix Project* was seized within days.

And the clampdown intensified still further. On March 1, the offices of Steve Jackson Games, a publishing company in Austin, were raided by the Secret Service. According to the Associated Press, the home of the managing editor was also searched. The police and Secret Service seized books, manuals, computers, technical equipment, and other documents. Agents also seized the final draft of a science fiction game written by the company. According to the *Austin American-Statesman*, the authorities were trying to determine whether the game was being used as a handbook for computer crime.

Callers to the *Illuminati* bulletin board (run by Steve Jackson Games), received the following message:

"Before the start of work on March 1, Steve Jackson Games was visited by agents of the United States Secret Service. They searched the building thoroughly, tore open several boxes in the warehouse, broke a few locks, and damaged a couple of filing cabinets (which we would gladly have let them examine, had they let us into the building), answered the phone discourteously at best, and confiscated some computer equipment, including the computer that the BBS was running on at the time.

"So far we have not received a clear explanation of what the Secret Service was looking for, what they expected to find, or much of anything else. We are fairly certain that Steve Jackson Games is not the target of whatever investigation is being conducted; in any case, we have done nothing illegal and have nothing whatsoever to hide. However, the equipment that was seized is apparently considered to be evidence in whatever they're investigating, so we aren't likely to get it back any time soon. It could be a month, it could be never.

"To minimize the possibility that this system will be confiscated as well, we have set it up to display this bulletin, and that's all. There is no message base at present. We apologize for the inconvenience, and we wish we dared do more than this."

Apparently, one of the system operators of *The Phoenix Project* was also affiliated with Steve Jackson Games. And that was all the authorities needed.

Raids continued throughout the country with reports of more than a dozen bulletin boards being shut down. In Atlanta, the papers reported that three local LOD hackers faced 40 years in prison and a $2 million fine.

Another statement from a Legion of Doom member (The Mentor, also a system operator of *The Phoenix Project*) attempted to explain the situation:

"LOD was formed to bring together the best minds from the computer underground - not to do any damage or for personal profit, but to share experiences and discuss computing. The group has *always* maintained the highest ethical standards.... On many occasions, we have acted to prevent abuse of systems.... I have known the people involved in this 911 case for many years, and there was *absolutely* no intent to interfere with or molest the 911 system in any manner. While we have occasionally entered a computer that we weren't supposed to be in, it is grounds for expulsion from the group and social ostracism to do any damage to a system or to attempt to commit fraud for personal profit.

"The biggest crime that has been committed is that of curiosity.... We have been instrumental in closing many security holes in the past, and had hoped to continue to do so in the future. The list of computer security people who count us as allies is long, but must remain anonymous. If any of them choose to identify themselves, we would appreciate the support."

> *"No member of LOD has ever broken into another system and used any information for personal gain."*

And The Plot Thickens

Meanwhile, in Lockport, Illinois, a strange tale was unfolding. The public UNIX system known as *Jolnet* that had been used to transmit the 911 files had also been seized. What's particularly odd here is that, according to the electronic newsletter *Telecom Digest*, the system operator, Rich Andrews, had been cooperating with federal authorities for over a year. Andrews found the files on his system nearly two years ago, forwarded them to AT&T, and was subsequently contacted by the authorities. He cooperated fully. Why, then, was his system seized as well? Andrews claimed it was all part of the investigation, but added, "One way to get [hackers] is by shutting down the sites they use to distribute stuff."

The *Jolnet* raid caused outrage in the bulletin board world, particularly among administrators and users of public UNIX systems.

Cliff Figallo, system administrator for *The Well*, a public UNIX system in California, voiced his concern. "The assumption that federal agents can seize a system owner's equipment as evidence in spite of the owner's lack of proven involvement in the alleged illegal activi-

(continued on page 34)

THE SECRETS OF MIZAR

by The "Q"

MIZAR is a Bell system used by the RCMAC (Recent Change Memory Administration Center), also known as the CIC in some areas. Its purpose is to process Recent Change Messages. Before we go into more detail, we will need to familiarize you with some terms.

First off, every Central Office (Wire Center, End Office, whatever) houses one or more switches, whether electromechanical, electronic (analog), or digital. Each switch is responsible for controlling various aspects of telephone service for one or more (usually more) exchanges. Switches in general can be classified into two main types: mechanical and SPCS. Thusly, SCC's (Switching Control Centers) are divided into separate branches. There are the E & M SCC (electromechanical) and the SPC SCC, which handle Stored Program Control Switches. The latter are computer controlled by software, whether they are older versions such as the 1 or 1A ESS (which use crossbars to complete calls) or digital switches such as the 5ESS or DMS100. Henceforth in this article, we will refer to SPCS switches as "electronic" switches, whether analog or digital.

MIZAR is a fortress containing a wealth of resources.

Basically speaking, a switch's memory can be thought of in three main parts: Call Store (CS), Program Store, and Recent Change. In general, a Recent Change Message is a batch of commands which tell the switch to perform an action on a facility (a TN, an OE, TRKGRP, etc.) The Program Store can be thought of as "ROM" memory. This program controls things behind the scenes such as interpreting and processing your commands, etc. Usually at the end of the day, Recent Changes which were processed that day are copied into the Call Store, which is a permanent memory storage area, somewhat "finalizing" the Recent Changes (although they could always be changed again). The 5ESS is similar to this, though it has many operational differences in processing Recent Changes, and Recent Changes are called "SERVORD's" on DMS machines and go into tables when processed.

Now that you are somewhat familiarized with some basic terminology, we will proceed in describing the operation of the MIZAR system. Like we said earlier, MIZAR processes Recent Change Messages (orders), which can be computer generated (by COSMOS, FACS flow-thru, etc.) or manually entered by the CIC. CIMAP (Circuit Installation Maintenance Assist Package) is a sub-system used by both the frame technicians and CIC. "CIMAPs" are primarily generated for new connection (NC) type orders. At the CIC there are three main types of orders processed: changes on a facility, snips, and restorals. Changes could be, for instance, modifications of line attributes. Snips are complete disconnects (CD's) which must be carried out on a switch in order to complete a CD type order. "Snip" is a term referring to what was done at the frame, i.e. a cable and pair's termination at the CO was "snipped" from the frame, hence a disconnect. "Restoral" is just the opposite of a snip. A cable and pair is being "restored", i.e. reconnected to the frame, and must now be activated at the switch and will hence be in-service once again.

On the average, a single MIZAR system handles Recent Change processing for about 20 switches (and it can handle more than that).

Every day, MIZAR logs into COSMOS automatically, usually at the end of the day, to retrieve Recent Change Messages which must be carried out in order to complete a pending service order. COSMOS takes a service order, and based on what is required, is able to generate an RCM from its tables in /usr/rcmap (on PDP-11's) or /cosmos/rcmap (on 3B20S or Amdahl's) which provides COSMOS with information concerning what type of switching equipment is associated with the wire center in effect and uses these tables to create the RCM accordingly. There are four main commands on COSMOS associated with Recent Changes. They are: RCS (to obtain a Recent Change Summary), RCR (to obtain a Recent Change Report), which would allow you to display an RCM if one was associated with a specific service order (all based on the filter options you specify for the search), RED (Recent change EDitor), which allows you to edit a Recent Change Message pending, and lastly, RCP (Recent Change Packager), which generates an RCM for one or more service orders to be processed by MIZAR.

After MIZAR retrieves RCM's from COSMOS, etc. it connects to the desired switch's recent change channel and the message is processed on the switch. MIZAR can connect to switches in various ways, depending upon its configuration. Switches may be accessed on dialup lines, X.25, or by dedicated hardwired connections. Switches can be accessed for the purpose of manually processing service orders with the ONS command. Once on the desired switch, it would be proper to utilize the RCM processing service provided through the MIZAR software, which will cause the service order to be properly logged to MIZAR's switch log (located in /tmp/swXX.out, where XX is the numerical code assigned to that switch), so that all will be up to date and accurate. However, if the RCM is entered straight onto the switch without letting MIZAR's log know, then an "unaccounted for" RC will be processed without ever being logged (except of course on the switch's rollback). COSMOS can be manually accessed with the ONC command. Orders can be queued and have their statuses checked with the ORI/ORS/VFY/etc. commands.

The coupled power of COSMOS and a small army of switches to do your bidding is a treasure worth its weight in gold.

When one first logs into MIZAR it

WHAT MIZAR CAN DO

should be noted that the login would be RCxx or RSxx, where xx represents the account number belonging to that specific RCMAC (CIC). For example, RC01, RS02, etc. Passwords, of course, could be anything within the standard Unix eight character limit. After receiving a login message, you will be prompted with an "SW?" and a "UID?". SW stands for what switch you wish to be logged in as (i.e. once logged in, any transactions would be reflected upon that actual switch). Hitting "?" will provide you with the list of switch identifiers available. They can be two letters (like on COSMOS) or more (which is usually the case, as part of the identifier indicates the type of electronic switch).

The UID must be a valid three letter code which would authorize that particular user to perform transactions with the desired switch. Typical UID's to be aware of are "all" and "any" which usually will work in conjunction with any switch you try to log in under. SW and UID must be provided for the purpose of setting up environment variables used by the MIZAR software. This is done in your .profile.

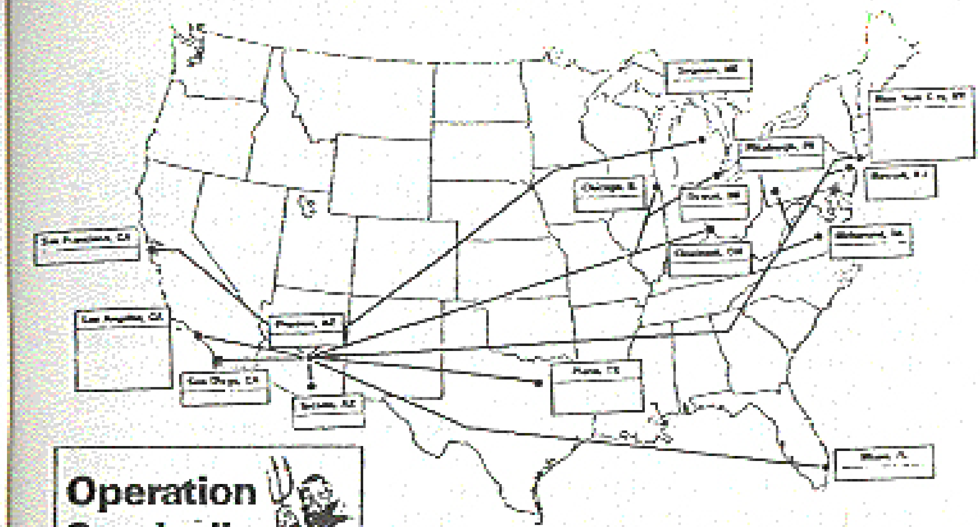
The typical MIZAR user's commands are located in the path /mms/mms (and are all three letters long). It should be noted that CFS on MIZAR is meant to be accurate and up to date with COSMOS'.

Some useful MIZAR commands are: MAR, which lists a MIZAR Activity Report, telling you what MIZAR's up to. MAB, Manually Adjust Blackout periods, is an important command. In some areas, MIZAR classifies switches as being in a "blackout period" at a certain time late in the day (usually the evening), as probably no one would be on that late, or possibly work is being done on the switch. Establishing a blackout period disables normal users from accessing a particular switch from MIZAR. On the other hand, MAB can be used to ENABLE a switch, and remove it from the blackout state. However, the CIC usually closes at 6PM (sometimes staying open as late as 9PM), and logins at such a late time would be foolish as you may jeopardize your future access. SDR, for Switch Data Report, allows you to list out useful information about the switches you specify — for instance, the NPA and exchanges this particular switch handles (including thousands of groups of DID and IBN blocks), its WC name on COSMOS, its configuration as a FACS/SOAC machine, MIZAR's times to call COSMOS, any preset blackout periods, whether AIS or E911 is available to the switch, all valid UID's for login to MIZAR, and usernames and/or passwords for switches that require them (such as the 5ESS or DMS100), as well as other useful information. WCH (Wire center CHange) allows you to change to another wire center (hence, further transactions apply to that wire center).

As you may have noticed from this article, MIZAR is a very useful system indeed. It's a fortress containing a wealth of resources. The coupled power of COSMOS and a small army of switches to do your bidding is a treasure worth its weight in gold.

This article was meant to familiarize the reader with the MIZAR management system. We welcome any questions you may have, and we will take pride in providing further articles on similar Bell systems and subjects, so as to better inform the curious mind.

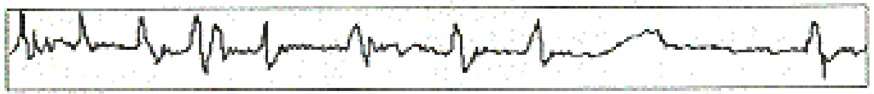
Bart Simpson is one rad dude.



Operation Sundevil

As we went to press, the largest hacker raid in history started happening. There aren't many details we can give you in this issue except to say that this is the first one we know of that had a name. 150 Secret Service agents were involved and tens of thousands of disks have been seized. This is all in addition to the raids spoken of elsewhere in this issue. Look for more details on this in the summer issue. And feel free to send us clippings from your local papers.

These are the brain waves of a normal American teenager.



These are the brain waves of the same teenager after hacking.

When you hack, you're overusing your brain
and are liable to find out things you shouldn't.

THE PARTNERSHIP FOR A HACKER-FREE AMERICA

toll fraud detection techniques

Here is an example of the truly horrible activities the Legion of Doom engaged in. An educational article such as this is a most dangerous weapon indeed, particularly from the standpoint of those who want the workings and capabilities of technology kept secret.

by Phantom Phreaker
and Doom Prophet
Legion of Doom!

There have been many rumors and false information going around about how phone phreaks are caught for using blue boxes. The purpose of this article is to dispel the rumors and myths circulating about this topic.

When a person attempts to access the telephone network with a blue box, they first must have an area that they can use to gain access to an in-band Single Frequency (SF) trunk. This is done by dialing direct or through a long distance service. At the appropriate time, the person sends a 2600 Hz tone through the telephone where it is registered by the terminating switching equipment as a disconnect signal. The terminating switching equipment or trunks leading to this office will be reset if they recognize the 2600 Hz tone. The effect of doing this is a wink, or an interruption in circuit. A wink is heard after the person sends 2600 Hz, and it sounds like a quiet "chirp" or sometimes a "kerchunk". From here, the person can signal to a trunk with Multi-Frequency tones in specific formats, depending upon what the user wished to accomplish. Each time the user sends 2600 Hz, the trunk will be reset and will send a wink back toward the user. AT&T calls these winks "Short Supervisory Transitions" or SST's.

If a person's central office equipment is a Northern Telecom DMS switch or an AT&T ESS switch, the SST caused by the 2600 Hz will be detected at that office and an output report will be issued from that specific switching system. In No. 1 and No. 1A ESS switches, these reports are called SIG IRR reports, or "SIGnal Irregularity" reports. They will be output with the appropriate information relating to the subscriber who initiated the SST. A sample SIGI report from a No. 1A ESS switch is included for an example.

```
*32 SIG IRR 69      0               00000
    000 555 1111  B8**3*BBBBBBBBB
```

We are unfamiliar with the details of these reports, but in this case, 555 1111 seems to be the Directory Number that originated the SST. Suffice it to say that these reports do exist and that they do help detect people trying to use blue boxes. SIGI is a *standard* feature in all 1A ESS machines. We're not sure about No. 1 ESS, but nearly all the other ESS machines most likely have SIGI or something similar to it.

In the case of NTI's DMS-100 switch, the feature is called "BLUEBOX". The BLUEBOX feature in DMS-100 is not standard. It can be implemented only by telco personnel activating it via a MAP (Maintenance and Analysis Position) channel. The DMS-100 reports are more detailed than the 1A ESS reports, possibly due to the fact that the DMS-100 switch is much newer than the 1A. DMS will recognize the trunk wink and then output a report. The system further checks for the presence of MF tones. If the MF tones are present, and are followed by an ST signal, another report is then generated by the switch. The calling number and called number (in MF) can then be recorded on AMA tape for further investigation by security personnel. In areas with past instances of toll fraud (blue box usage) and in major cities, it can be assumed the BLUEBOX series of features would be implemented. In rural and small town areas, there is less of a chance of this feature being present. The plain fact that this feature exists should be enough to keep you from trying anything foolish.

Since most electronic/digital switching systems have provisions in them to catch blue boxers, one may wonder how to box safely. The safest method of blue boxing would be to not let an SST show up on your line. This can be accomplished by boxing through a long distance service via dialup (Feature Group A or B). The only catch is that the long distance service that you use must not send back a wink when you attempt to box over its network. If an FG-B accessible trunk running from a toll office to an alternate carrier's facilities recognizes your 2600 Hz tone and disconnects, then SIGI or BLUEBOX would indicate your existence and you could be punished for your crime. So, if you must try such things, they are best done from someone else's line or from a coinphone.

STAFF

Editor-In-Chief
Emmanuel Goldstein

Artwork
Holly Kaufman Spruch

Photo Salvation
Ken Copel

Design
Zelda and the Right Thumb

Writers: Eric Corley, John Drake, Paul Estev, Mr. French, The Glitch, The Infidel, Log Lady, The Plague, The Q, David Ruderman, Bernie S., Lou Scannon, Silent Switchman, Mr. Upsetter, Violence, and the faithful anonymous bunch.

Remote Observations: Geo. C. Tilyou

BUILDING A DTMF DECODER

by B/Square
and Mr. Upsetter

Imagine this scenario: you are listening to your scanner, monitoring a neighbor using his cordless phone. He is accessing his bank-by-phone account. He enters his password, and you hear the whole thing. But the only problem is that he entered the password using touch tones. How do you know which numbers he entered?

Or think of this: you're doing an investigation and recording telephone calls. The person under surveillance is making calls with a touch tone phone and you have tapes of everything. But how do you find out what numbers were dialed?

One answer to these problems would be to buy a commercial DTMF (touch tone) decoder or a similar device called a pen register. These items could cost you a few hundred dollars. The other solution is to build the handy "snatch 'n latch" DTMF decoder presented here for about $35 to $45.

This circuit uses a single chip to decode 12 or all 16 DTMF tones, as selected by the user. Up to 16 tones are stored in the circuit's static RAM memory. Once the tones are in memory, the user reads them out one by one on the circuit's LED display. The circuit can be hooked up to a telephone line, a scanner, or a tape recorder. Now let's take a look at how this little device works.

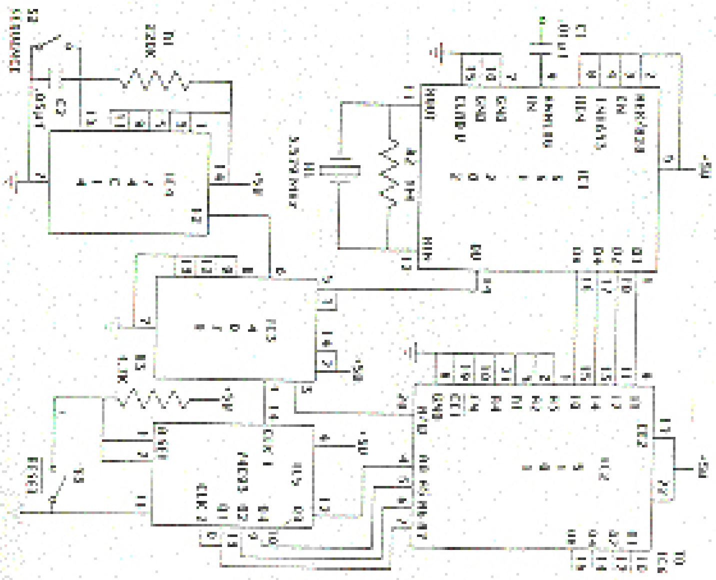
Theory of Operation

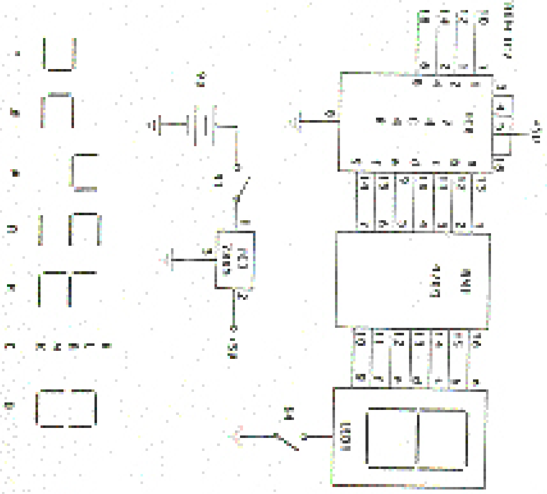
DTMF signals are coupled to pin 9 of IC1, the DTMF decoder chip, by .01 uf capacitor C1. The tones are band split sampled and a coded output is placed on D1, 2, 4, 8, of IC1. Data valid (pin 14) goes high 7 usec. after data is on bus causing the R/W input of the RAM, IC2, to go low and the CLK1 input (pin 14) of the counter, IC5, to go high by way of IC3, the XOR. At this time, the digit received is displayed on LED1 while preconditions (to write the data to memory) are established. 45 msec. after the tone ends, DV goes low, writing the data into RAM and incrementing the counter one count. Code has been written into address 00 of the RAM with the next address presented to A0, 5, 6, 7 of the RAM. 4.56 msec. after DV goes low, the outputs D1, 2, 4, 8 of the decoder clear. This sequence will continue until addresses 00 through 15 contain data. At this time, the counter recycles and data will be written over what was previously stored.

To read out the contents of memory, S3 is opened, causing pins 1 and 2 of the counter to go high. This resets the counter address bus to 00. The data in address 00 of the RAM is presented to IC6, the BCD to 7-segment driver. IC6 converts the RAM output data to a digit which is read out on LED1. When S2 is closed, pin 12 of IC4, the Schmitt trigger, goes high. This causes pin 14 of the counter to go from low to high by way of the XOR. This increments the counter and presents the next address to the RAM, and the next digit is read out. S2 is repeatedly pressed until all the contents of memory have been displayed.

Circuit Construction

There are two different tech-





niques you can use to construct your own DTMF decoder. These are wire wrap and soldering. In fact, before you decide to build a permanent unit, you may want to put the circuit together on a plastic breadboard. The authors have built units in these three ways and they all worked equally well.

There are some important things to consider before you start. It is very important that you take some time to figure out where you are going to place the IC's to facilitate a "clean" project. This means, for example, that you shouldn't put IC1 on the opposite side of the board from IC2 because they have a data bus running between them. This may get complicated, but it is important to figure out a good parts layout before you start soldering things together. Also, it is a good idea to buy all the parts, including PC board, enclosure, sockets, switches, etc. before you get started on a permanent unit so you can plan how you are going to put everything together. In addition, unless you are a soldering whiz, it is highly recommended that you use sockets for all the IC's. This also makes troubleshooting the device and replacing IC's easier.

This project uses CMOS IC's, which are static sensitive. Theoretically you and your soldering iron should be grounded when handling the IC's. If you don't have an anti-static workstation handy, don't worry about it too much. Try not to touch the pins of the IC's and store them in conductive foam or a piece of tin foil when not in use.

Assembly is readily achieved using 30 gauge hand wire wrap on the back plane of a "universal" PC board (available from Jameco, Radio Shack). Once the layout of the IC's is determined, solder two opposing pins of each socket to the board and methodically wire pin to pin keeping in mind that the pinout is reversed on the wiring side of the board. The crystal can be mounted horizontally or vertically, but the 7805 regulator should be mounted horizontally for low profile. The 30 gauge wire is soldered directly to the switches and jack. Doublechecking your work at various stages will assure a functional device at power-up. Before you insert the IC's into the sockets, check all connections with a continuity meter. Should the circuit not operate, suspect your work before questioning the IC's. The advantage of wire wrap is that it is easier to correct your mistakes.

Assembly by soldering is quite similar to wire wrap. A board with a pattern such as Radio Shack p/n 276-162 is recommended. Solder the IC sockets to the board once you decide on a good layout. Solder the other parts in place. Solder small gauge wires from pin to pin on the component side of the board. Use small jumpers made from component leads for short connections on the component side and the solder side. Check all connections with a continuity meter.

When you put the IC's in their sockets, remember to put them in the correct way, not backwards.

As good circuit design practice you may want to put .1 uf capacitors between the power supply pins of each IC and ground. The device will work without them, however.

After you are done with the PCB, think about where you are going to put the LED display, input jack, and switches on your enclosure. Assembly and disassembly will be easier if all of these things are attached to one half of your box.

Using the Decoder

Using the "snatch 'n latch" isn't too hard, but there are a few details about its operation that we need to observe. When you first turn the unit on, be sure to hit the reset switch. This ensures that the tones (or rather the data sent from the decoder to memory) will be stored in the first memory location. Then you sit back and wait for some DTMF tones to come down the line. When they do, the device will snatch 'em and stash 'em in the memory. When the tones have stopped, hit the reset switch. You will see a number on the display, which is the number stored in the first memory location. Hit the sequence button and the numbers in the subsequent memory locations will be read out. Once you've read out all the numbers and written them down somewhere, hit the reset switch again. You are ready to start all over again. The numbers will be in memory as long as the power is on and new numbers haven't been written over the old ones. (That's why you may want to write down the numbers, because any new numbers that come in will erase the old ones.)

There are a few other helpful hints that can make using the decoder easier. First of all, install that switch to turn the LED display on and off. You only need the display when you're reading out numbers, and switching it off will prolong battery life. Also, while reading out the numbers, you might want to remove the device from the phone line or whatever it is hooked up to. If the decoder happens to receive a tone while you're reading out the numbers in memory, the tone will be stored in whatever memory location you happen to be at and generally make things confusing.

One feature of the "snatch 'n latch" that makes it less attractive than commercial models is that it can only store 16 tones. If more than 16 tones are read by the decoder, the counter resets the RAM to the first memory location and the excess tones are read into memory, erasing the previous ones. This is a problem since information is lost. If you anticipate reading in more than 16 tones at one time, you can record the tones on tape and play them back a few at a time into the decoder.

When using the decoder with a tape recorder, hook it up to the earphone jack and adjust the volume so the decoder will read the tones off the tape. The decoder isn't terribly picky about input levels, but theoretically the input level should be less than the supply voltage, which is 5 volts DC. When using the decoder with a scanner, it's best to hook it up to a "tape out" jack if it has one.

Otherwise you can hook it up to the earphone jack. The decoder works like a charm when hooked up directly to a phone line (parallel connected), as the capacitor on the input of the DTMF decoder IC blocks the phone line's DC voltage. However, if you are going to hook up the "snatch 'n latch" to the phone line for any extended period of time, circuitry must be added to the input to protect the device from the ringing voltage. 90 volts AC on the line will surely wreak havoc on the CMOS IC's.

Applications

The DTMF decoder has many interesting uses. Basically, anytime you hear a tone and want to know what it is, hook up the decoder and let it go to work. When it is hooked up to a phone line, the number dialed can be decoded. You can also decode DTMF tones (e.g. passwords) used for services like bank-by-phone, credit card verification, voice mail systems, etc. Calling card numbers can be obtained in the same way if they are entered by touch tone. If you monitor cordless or cellular phones with a scanner, you can hear a lot of this type of DTMF tone use. With a scanner you can also decode such things as access tones for repeaters. DTMF signaling is so widespread there's no doubt that you will discover other useful applications.

The "snatch 'n latch" DTMF decoder presented here is a cost-effective circuit that is an invaluable tool for the telephone experimenter. We hope this article will start you on your way towards building your own.

Parts List

C1- .01 uf
C2- .05 uf
R1- 220K, ohm, 1/4 watt
R2- 1M ohm, 1/4 watt
R3- 4.7K ohm, 1/4 watt
RN1- 470 ohm
X1- 3.579 MHz colorburst, HC-18 case
S1, S4- SPST switch
S2- momentary, normally open
S3- momentary, normally closed
LED1- 7 segment, common cathode
IC1- SSI202, DTMF decoder
IC2- 5101, 256x4 SRAM
IC3- CD4070, quad XOR
IC4- 74C14, hex schmitt trigger
IC5- 74C93, ripple counter
IC6- 74C48, BCD to 7-segment
IC7- 7805, 5V regulator
Misc. parts: 1/8 inch jack, IC sockets, PC board, 9V battery and clip, .1 uf capacitors, enclosure, mounting hardware.

All of the IC's except for IC1 are available from Jameco Electronics, 1355 Shoreway Road, Belmont, CA 94002 (415) 592-8097. They also have sockets, the crystal, and other parts. Some parts are also available from Mouser Electronics. Call 800-992-9943 for a free catalog. The SSI202 DTMF decoder IC is available from W.E.B., PO Box 2771, Spring Valley, CA 92077 for $12.95 plus $2.50 postage and handling.

SILVER BOX BORN IN U.K.

by Tamlyn Gam

There was an article about the construction of a silver box in the Winter 1989/90 issue and it led me to wonder how this would work in the United Kingdom and Europe.

Much of the UK is still using pulse dialing and the use of tone phones is only just spreading. (Most still convert the tone to a pulse for the sake of the antiquated phone system.) As the use of tone systems spreads, now at an increasing pace, there would seem to be a rich area for experiment here. It is not easy to come across a tone phone over here so I had to look for another source for the box parts. The main use here of tones is to control remote devices over telephone lines. These services which are common in the US are only just beginning to come into general use here, but we are now able to use tone controlled answerphones and tone controlled services such as voice banks and bank services. With the lack of tone exchanges and phones, the suppliers of such services have been offering small tone generators to prospective customers (sometimes free). Any hacker worth his salt will have one or three.

I dug out one of mine and pulled it to pieces and, yes, it was run by a 5087 chip. A quick look at the circuit showed it to be the same as the phone described in the earlier article, so I fitted a changeover switch as suggested and am now the proud owner of a silver box.

I am not sure just what I can do with it but time will tell. The received wisdom is that the extra tones are not used in the UK, but I see that the telephone workers are equipped with tone generators having 16 buttons. An "innocent" question as to what all those extra buttons were for has not yet yielded results — but it will. In the meantime I will poke the extra tones about to see what they do and report back. I do work in an office with an internal tone phone service with national links to the public network so I have lots of places to experiment. I will report back here and in the meantime will see what our US colleagues turn up as they blaze the trail.

LISTENING IN

by Mr. Upsetter

Every now and then, those of us who take the time to be observant stumble across something remarkable. Let me relate to you one of those experiences. It was an all too lazy sunny afternoon in Southern California. I was bored, and I decided to listen to my Realistic PRO-2004 scanner. I flipped it on and scanned through the usual federal government, military aviation, and cordless phone frequencies, but there was no good action to be found. I happened across some scrambled DEA transmissions and a droning cordless phone conversation by some neighbors I could not identify. So for a change I scanned

LISTENING TO PHONE CALLS ON THE RADIO

A reader tells us:

"Be advised that cordless phones are quite easy to monitor, and yours is just as accessible to eavesdropping as anyone's. But there's a hidden danger with some cordless units — they may be transmitting your personal conversations even when not in direct use! This occurs with our newish General Electric System 10, model 2-9675.

"I discovered this "feature" one day when my wife called home while my scanner was whizzing away between 40-50 MHz. I answered on the wired office phone at my desk, with the cordless remote unit hung on the wall on the far side of the kitchen and its base unit cradled in the bedroom. Suddenly, our voices echoed throughout the room! The scanner had hit the 46.xxx MHz frequency the base unit uses to transmit both sides of the conversation and was functioning as a wireless speakerphone!

"I should emphasize that anything you disseminate on any phone circuit may be monitored by someone — the cordless phone just increases the number of possible intercepts, and lowers the level of expertise required to violate your privacy."

through the marine radio channels.

The scanner stopped on marine radio channel 26, which is used for ship-to-shore telephone calls. A man was reading off his calling card number to the operator, who gladly accepted and connected his call. Calling card numbers over the airwaves! I was shocked — astonished that such a lack of security could not only exist, but be accepted practice. I began monitoring marine telephone to find out more, and it turns out that using a calling card for billing is commonplace on VHF marine radiotelephone.

People use calling cards for billing all the time. That's what they are for. But is it that big of a deal? You bet it is. Marine telephone uses two frequencies, one for the ship and one for the shore station. The shore station transmits both sides of the conversation at considerable power, enough to offer reliable communications up to 50 miles offshore. Anyone with a standard police type scanner costing as little as $100 can listen in. People using marine radiotelephone can be broadcasting their calling card number to a potential audience of thousands. And that just shouldn't be happening.

But it is. And there is no doubt that calling card fraud is occurring because of this lack of security. From the phone company's (many Bell and non-Bell companies provide marine telephone service) point of view it must be a trade-off for customer convenience. You see, there just aren't that many ways to bill a ship-to-shore call. Most calls are collect, a few are billed to the ship if they have an account, and a few go to third party numbers or other special accounts.

Sometimes the operators have trouble verifying billing information. I monitored one man, who after racking up $40 worth of AT&T charges was informed that they couldn't accept his international account number. The operator finally coaxed him into giving an address for billing. Calls are often billed to third party numbers without verification. But calling cards make billing easy for both the customer and the phone company involved.

It would also be tricky for a company to not allow calling card use. Doing so would be an inconvenience to customers and would force them to admit a lack of communications security. Of course people using marine radio should already realize that their conversations aren't private, but announcing the fact wouldn't help the phone company at all. In fact, people may place less calls.

The convenience offered by calling cards makes them an easy target for fraud. They can be used by anyone from any phone and with a variety of different long distance carriers via 10XXX numbers. No red or blue box hardware necessary here, just 14 digits. But of course, the number won't be valid for long after all those strange charges start showing up on someone's bill. It should be noted that when a calling card is used, the number called, time and date of call, and location (and often, the number) from which the call was placed are printed on the bill. A fraudulent user could be caught via that information if they were careless. Also, some long distance companies may contact the owner of the card if they notice an unusually high number of charges on the card.

Long distance companies bear the brunt of the bills caused by calling card fraud. However, if you read the fine print, the cards offered by many companies have a certain minimum amount that the customer must pay, say $25 or $50. (Editor's note: We have yet to hear of a case where a phone company got away with charging a customer when the only thing stolen was a number and not the card itself.)

So what's the moral of the story? Simple. *Be damn careful what you say over any radio*, and that includes cordless and cellular telephones. If you are using a calling card, enter it with touch tones. If you happen to make VHF marine radiotelephone calls, bill collect or charge to your phone number as you would to a third party number — without the last

(continued on page 33)

THINK OF WHAT YOU COULD DO WITH $20,000.

That's the amount of money you'll save if you buy the much heralded E911 documentation from us instead of through Bell South. While they've priced this six page document at $79,449, we'll give it to you for only $59,449!* That's a savings of over 25%.

Imagine the thrill of owning a phrase like: "When an occasional all zero condition is reported, the SSC/MAC should dispatch SSIM/I&M to routine equipment on a 'chronic' troublesweep." (Those words by themselves would easily sell for several hundred dollars.)

You know that offers like this aren't made very often. You also know that this kind of information is a treasure well worth dying for which can't be found in stores anywhere. It's a commonly known fact that understanding how the phone company works is a major step towards World Conquest.

So take that step today. Before your neighbor does....

MAKE CHECKS OUT TO "2600 UNBELIEVABLE OFFER". (AVOID SENDING CASH THROUGH THE MAIL.) THIS OFFER ENDS JULY 31.

* DOES NOT INCLUDE TAX AND SHIPPING.

```
# bigcheese (Internet scanner in shell)
#
# When run off a Unix with Internet access, this program will scan for ALL
# computer systems tied to the network.  Telnets will be placed in a file
# called .UNIXES
# A complete listing of systems (including both Unixes and non-Unix based
# systems will be found in .all.systems
#
# Please note: This is a "simplified" version written in approximately 1 hour.


if [ -z "$4" ]; then
echo "\nUsage: big.cheese xxx xxx xxx xxx"
exit
else
prefix=$1;addr1=$2;addr2=$3;addr3=$4
fi
export prefix addr1 addr2 addr3
while :
do
if [ -f /tmp/stop.scn ]; then
break
fi
echo "\r\n\r\n\r\n" | telnet "${prefix}.${addr1}.${addr2}.${addr3}" >/tmp/.chkit&
sleep 10
kill 0
cat /tmp/.chkit >> .all.systems
a=`grep "login:" /tmp/.chkit`
          if [ "$a" ]; then
          echo "`date` => ${prefix}.${addr1}.${addr2}.${addr3}" >> .UNIXES
          fi
if [ $addr3 -gt 255 ]; then
          addr2=`expr $addr2 + 1`;addr3=0
                    if [ $addr2 -gt 255 ]; then
                    addr1=`expr $addr1 + 1`;addr2=0
                                        if [ $addr1 -gt 255 ]; then
                                        break
                                        fi
                    fi
fi
done
```

WE GET THE MOST INTERESTING FAXES FOR MILES AROUND.SEND YOURS TO 516-751-2608 ANYTIME.

news update

Morris Sentenced

On May 4, Robert Morris, whose runaway worm created havoc on the Internet over the fall of 1988, was sentenced to three years' probation, a $10,000 fine, and 400 hours of community service. He could have received up to five years in prison along with a $250,000 fine.

While it seems pretty strange to sentence somebody for what was, in effect, a scientific experiment gone awry, it certainly is a relief that cooler heads seemed to prevail in this important case. After all, Morris could have wound up in prison. We can only hope this isn't the exception to the rule, or worse, a case of special treatment because his father works for the NSA.

Albania Callable

For many years, the strange and mysterious European country of Albania was completely unreachable by telephone, at least from the United States. But all of that suddenly changed on May 1, when AT&T started providing operator assisted calls there. It's rumored that direct dial service will start in the fall. If so, the country code is 355. The call shown below was made from Canada. Now there are only three countries that are unreachable from the United States: Vietnam, Cambodia, and North Korea. (Actually, it IS possible to call those places from here - can you figure out how?)

No.	Date	Called from	Called to	Time	Rate	Min.	Amount
	Calling number 751-2600						
1	FEB 09	SOO ON 705 759-0000	ALBANIASPR	10 AM	PS PERSON	18	$28.60

MCI Insecurity

In an internal memo leaked to 2600, MCI admits that there is very little security for their international calling cards. The "international number" is defined as a 17 to 19 digit number composed of the Telecommunications Industry Identifier (89), the country code (from one to three digits), an MCI issuer identifier (222 or 950), the subscriber number (the same as the first ten digits of the MCI 14 digit domestic number), and a check digit. The international number is used when going through operators overseas, not when using MCI Call USA, the MCI equivalent of AT&T's USA Direct.

```
- MCI CONFIDENTIAL -
DO NOT SHOW CUSTOMERS
```

In a section on fraud, MCI states, "Because there will be no automated validation of the International Number, fraud is a potential issue. However, it should be noted that AT&T has operated this service for over 20 years without validation of its international number." That should paint a pretty clear picture of the effective and immediate solutions some companies come up with when faced with potential security problems.

New York Tel Rate Increase

New York Telephone is asking for some of the most outrageous rate increases in its history. Apart from lowering the nighttime discount rate to 50 percent (from 60 percent) and the evening rate to 25 from 35, the company plans to double the charges for most classes of message-rate service. For instance, if you pay $8 a month for a certain type of service, you can look forward to paying $16 or more in the future. Not only that but charges to local directory assistance from payphones (currently free) will be initiated at a cost of 50 cents per request. The two free requests every customer gets each month will be eliminated. And an unprecedented 50 cent charge will apply to all calls to the operator that don't wind up in a call being processed! The Public Service Commission can deny the rate increase, but if they don't, these outrageous rates will go into effect next January.

Furthermore...

US Sprint has redesigned their bills. And, if you have a 950 access code, you'll be delighted to know that they print your code on every page!

you've found the official 2600 letters column

Clarifying REMOBS

Dear 2600:

In reference to your REMOBS article by The Infidel in the Autumn 1989 issue, the author distorted the true definition of Remote Observation in the digital age.

The REMOBS is a hardware device manufactured by TelTone and numerous other electronics manufacturers. To say that,it is a Bell standard piece of equipment could not be further from the truth. A typical REMOBS ranges in cost from $800 to $1200 and is always attached to the cable and pair in question at the frame (in the central office). The fact remains that the REMOBS is not totally silent. It is a mechanical device that uses cross-connect circuits to tap into a line, which obviously results in clicks and noises. Unlike The Infidel's notion that a REMOBS can monitor any line in an exchange, it is limited to a minimal number of subscriber lines and is restricted to guidelines set forth by the FCC. Ma Bell uses a series of circuits known as "no test trunks" to monitor lines for testing, and linemen in particular use software driven monitoring devices (TV on LMOS). Whether or not the observer will be heard depends upon the software selection.

To say you don't actually "connect" to a customer's line and simply monitor it is totally wrong. It is impossible to listen in on a conversation if there is no physical connection to the remote line you wish to observe (with the exception of cellular and cordless, etc.).

MOD!
Masters of Deception
New York City

And don't forget satellites and microwave links. It's quite a bit harder to zero in on a particular conversation but there's also a lot more to choose from with virtually no chance of being caught. In addition, DMS-100 switches seem to be gaining a reputation for inadvertently allowing access to other conversations. The story is always the same: you're having a conversation and all of a sudden you're connected to another conversation. You can hear them but they can't hear you. They hang up and you get another conversation. And so on. If there are "clicks" in these instances, nobody seems to be hearing them. Which brings us to an interesting point. If there are telltale sounds involved, how many of us know what they mean? Is every click on our lines someone eavesdropping? Of course not. Are monitoring devices becoming more sophisticated and less "noisy"? Absolutely. These facts, coupled with the increasing number of ways to listen, assures us of the fact that no phone conversation can be considered secure.

Who's Listening?

Dear 2600:

I am the victim of an "Information Source" that has me puzzled. My phones (according to Ma Bell) were not bugged and I know for a fact that no bugs were planted in my office. There was no illegal tap on my phone that I could detect.

Someone mentioned a new tap that is put into effect by just dialing my number. There is no ring and the listener can hear all that goes on in the room where the phone is. There is also no record of the phone call. This sounds like a combination black box and some other device.

Can you clue me in?

WH
Upstate New York

A harmonica bug, also known as an infinity transmitter, is usually placed in the earpiece of the phone. A particular frequency sent over the phone triggers them to start transmitting. If this was the case here, you should have been able to find it, although some have been made to look like phone jacks. Keep in mind that this is not a tap, but a bug. In other words, it works even when the phone isn't in use, monitoring the room, not the phone line. We're unaware of any "service" that allows someone to call in and do this without first having physical access to the phone. There are maintenance functions within the telephone company that allow lines to be monitored without having to install equipment, but these aren't supposed to be used outside the company. Somehow that doesn't sound very reassuring, does it?

Blue Box Chip

Dear 2600:

Although we are in the twilight of the blue box era, I'm sure many readers would be interested in an excellent blue box IC. The chip is the Teltone M-993 Multifrequency Tone Generator. It generates all 12 MF tones using a standard 3.58 Mhz colorburst crystal.

This chip offers several advantages to blue box designers. All blue box tones are generated accurately by one IC (except for 2600 Hz) and no adjustment or tuning is required. It does have one disadvantage, however. The IC has a 4 bit binary input for tone selection, meaning it isn't easily interfaced with a keypad.

The IC is also expensive, costing anywhere from $14 to $25 for single pieces. I have found two sources: High Technology Semiconductors in California (714) 259-7733 and Almo Electronics with outlets coast to coast (800) 525-6666. Other Teltone distributors sell it too. Teltone Corp. can be reached at (206) 827-9626.

Some distributors will give electronics companies free samples and spec sheets.

Mr. Upsetter

Bugs Wanted

Dear 2600:

If, as The Dark Overlord says, there are many weaknesses in UNIX, why don't you print a few? I frequently see messages on Arpanet saying things like "Major security bug found in XWindows, service representative will contact your site with details, disable XWindows until then" (no, this is not a real message), and there are evidently lots of administrators who know lots of easy-to-exploit bugs/holes in various op systems. Why don't you publish them? To

the first letters of the nineties

my knowledge 2600 has *never* published any specific security holes — not even the rhosts bug that the Worm exploited, which everybody except me seems to know about. For instance, Bill Landreth said he broke into a VAX running VMS using a rapid-fire command replacement: a program in C which submitted a command, waited until it was approved, and then wrote a different command into the VMS buffers before it was executed. Someone must have details: formats, specific memory locations, and timing — maybe a similar program.

I know people who have a .COM file on VMS which allows them to send mail messages with bogus "From:" fields. They are unwilling to supply me with it for fear of losing their jobs. Can someone provide a listing? How about ways of faking Arpanet mailer headings? (A practice very common on April 1)

I was recently on a VAX running VMS on which I had read privs for AUTHORIZE.EXE. I copied it into my directory, created a fake template of users, passwords, and privileges, and tried to redefine the appropriate logicals so that I could then SET HOST and login using my fake AUTHORIZE.DAT and get a bogus account pointed at a real directory with real privs. I had no success. Can anyone with access to VMS manuals tell if this is possible, and if so, what logicals to redefine?

Charlie Brown

Questions and Info

Dear 2600:

I have a lot to get off of my mind after reading your Winter 89-90 issue. I haven't had a computer for months now so I've been out of the phreak/hack scene for quite a while.

1. What are some of the ways that blue and red boxes can be used and detected on DMS-200 and other new switching systems?

2. When scanning (war-dialing), how many numbers per minute does it take to trip a warning flag at the CO?

3. Are test numbers called from a different area code billed?

4. Are there any other hack/phreak publications past or present?

5. Does anyone have, or has there been printed, a listing of Telenet Network User Addresses (NUA)?

6. What is the Summercon, as listed in the winter issue's Marketplace?

7. I have recently gotten my hands on an M-242A REMOBS unit. I have no idea what it does or how to work it. Any info will be appreciated.

Last of all, here are some interesting numbers in the 704 area code: ANI: 311, ringback: 340-xxxx. Here are some rather different COCOT numbers: 704-334-1051, 704-334-0745. These payphones, if not picked up within approximately 8 rings, will answer with a computer connect tone, followed in about 5 seconds by a very strange tone.

GB

First off, a DMS-200 is a toll switch, meaning it's used only for long distance switching and not in central offices. The #4 ESS is another example of this. Check elsewhere in this issue for details on how blue boxers are detected.

In some places, scanning has been made illegal. It would be hard, though, for someone to file a complaint against you for scanning since the whole purpose is to call every number once and only once. It's not likely to be thought of as harassment by anyone who gets a single phone call from a scanning computer. Some central offices have been known to react strangely when people start scanning. Sometimes you're unable to get a dialtone for hours after you start scanning. But there is no uniform policy. The best thing to do is to first find out if you've got some crazy law saying you can't do it. If, as is likely, there is no such law, the only way to find out what happens is to give it a try.

Test numbers will almost always bill when called from outside the area they're meant for. Sometimes they even bill locally!

We know of no other publication in this country that does exactly what we do, but there are some that have some similarities. When we find out about them and get ahold of a copy, we generally spread the word.

Getting a listing of Telenet addresses is like getting a telephone book. It would be outdated the moment you set eyes upon it. But there are many partial listings floating around, and if we get one in the future we'll share it as we've done in the past.

Re: Summercon, it's an annual gathering of American hackers and phreaks. The details will be announced when we have them.

Finally, the REMOBS unit you have will only work from WITHIN the central office. Those units are used for monitoring trunks, not individual lines, and they're really rather outdated. Still, it can't hurt to have one lying around the house....

Yet Another Threat

Dear 2600:

I think you might find this interesting. It was extracted from the RISKS Digest on USENET.

"The Prodigy Services publication, *Prodigy Star* (Volume III, No. 1) recently showcased a 'major benefit'. The Prodigy system accesses remote subscribers' disks to check the Prodigy software version used, and when necessary, downloads the latest programs. This process is automatic when subscribers link to the network.

"I asked Prodigy how they protect against the possibility of altering subscribers' non-Prodigy programs, or reading their personal data. Prodigy's less-than-reassuring response was essentially (1) we don't look at other programs, and (2) you can boot from a floppy disk. According to Prodigy, the fea-

2600 LETTERS, PO BOX 99, MIDDLE ISLAND, NY 11953 ture cannot be disabled."

I think it is obvious how to make use of this "feature" for other purposes. Let us hope that this "feature" is removed from one of the newly downloaded versions....

fin

Red Box Woes

Dear 2600:

Since the fonco strike in New York, the outdoor payphones that were vandalized and are now repaired do not allow red box usage. Even after putting in the first coin, using the box results in a recorded request to deposit the balance due. They must have done something with the coin detect relay setup. Indoor phones in building lobbies and stores still seem to work okay.

Curious

Throughout most of New York, a new relay system known as MARS has been installed over the last year. You may have noticed a difference in the way the dial tone appears. Some phones may not have been switched over yet. We're looking for more information on this, as well as ways of bypassing the disadvantages.

Dear 2600:

Your latest issue on building a silver box using a Radio Shack dialer was quite good. I would like to know if a modification can be made with a pocket Radio Shack dialer to build a red box.

Please reply by letter since I'm not sure if my subscription is expired.

Rhode Island

There wouldn't be much point to making a red box out of a Radio Shack dialer since a red box only makes a single combination of tones (1700 hz and 2200 hz). One 60 millisecond pulse indicates a nickel, two 60 millisecond pulses indicate a dime, and five 35 millisecond pulses separated by 35 milliseconds indicate a quarter. These tones are not found on a touch tone pad, whereas the silver box tones are. Our Summer 1988 edition has red box plans for those who are interested. It should be noted, though, that many red boxes are nothing more than tape recorders with the appropriate tones cued up.

There's no way we can reply individually to all of the questions we get. It's up to you to keep track of when your subscription is nearing an end. That information should be on your mailing label.

While we're on the subject, folks, a couple of words of advice. When you move, let us know BEFORE your old address becomes invalid. The post office does not forward magazines. Instead, they send us notification of your new address, a service they charge us for. And you wind up missing an issue for no good reason. Also, those of you using aliases: make sure you're able to get mail under that name. There is nothing more frustrating than trying to contact someone whose issues keep coming back to us, especially when they're complaining to us about not getting what they paid for! If you have to use a fake name or handle, just make sure the post office knows about it so we can all get on with our lives.

Suggestions and Questions

Dear 2600:

Glad to see your you covering phones again. Very much enjoyed the fortress phone article and had a few questions about it.

Green box tones: when are these tones to be sent? When you are still talking? After you hang up and pick up the phone again?

Red box or green box tones: do they have to be sine wave tones or will square wave tones work?

Just what are toll free 950 calls?

What is beige boxing and how is it useful? How about an article for remedials like me?

Redneck 1
San Luis Obispo, CA

Green box tones are simply MF tones used in a different way. For instance, KP is the signal to spit out the change. The MF number 2 is the signal to collect the coins. There are other tones for obscure functions which nobody really uses these days. Keep in mind that these tones are only used on analog switches. The tones must be sent from the called party. The person you call blasts KP, you hang up, and your change should come back, provided it hasn't already dropped.

Either sine wave or square wave tones work just fine.

950's are toll free numbers that provide you with access to the dial tones of other long distance companies. It's necessary to enter an authorization code before or after entering the number you want to call. These dial tones only accept touch tones, not pulse. 950-1022 belongs to MCI, 950-1033 belongs to Sprint, and there are many others floating around just waiting to be discovered.

Beige boxing is nothing more than using someone else's phone line to make a call. This is done quite a bit in dormitories, where it's fairly easy to get access to the phone closet and do some rewiring.

Dear 2600:

Keep up the good work. I like a balance between telephony and computers: software and hardware. The international info is valuable. You ought to combine this and one of the other magazines into a real, full-blown rag like Data Communications. How about a feature on the ATT System 75/85 PBX?

Satisfied Customer

We'll look into that PBX and see if there's anything particularly interesting about it. At the moment, we have little interest in looking or reading like Data Communications.

Dear 2600:

I have asked you before, but has any new information come up on publications similar to yours in the United Kingdom or the Netherlands? I admire your persistence and philosophy, and hope that you will continue for as long as you feel moved to do so.

An Overseas Fan

There has been talk of a publication starting in England for some time. We'll let you know if any-

letters for the spring of 1990

thing develops. In the Netherlands, there's Hack-Tic at PO Box 22953, 1100 DL Amsterdam.

Dear 2600:

Would you be interested in an article about computer viruses? I have an Apple, so everything concerning it would be based on Apple assembly language. The article would cover how to make, destroy, and detect viruses on the Apple, and in general. I might supply a simple source code for a non-destructive self-replicating program, if you are interested.

Somewhere in the Midwest

We're surprised you had to ask. We're waiting by the mailbox.

Hotel Phones

Dear 2600:

I recently came across a very major security problem when using private phone systems such as in hotels.

Most of these have a Station Message Detail Recorder (SMDR) which keeps track of all digits entered at your extension. At checkout time these numbers are compared, either electronically or by hand, with a rate chart and the bill gets calculated.

Since I generally use alternative common carriers for long distance calls, I almost always have a local, free (950) access number.

Recently, one institution tried charging me excessive amounts, claiming that I had accessed some of the other, ahem, special exchanges (anything above zero is wrong, but I'll grant them the 25 cents if they insist) so I asked to see the printout.

I discovered, to my very major dismay, that the paper had the 950 calling number *and* my security code, as well as the final number dialed.

On checking further, I discovered this is not only a common feature of SMDR's, but is also on many private coin phones.

Very curious, and very worrisome.

I found a way to (sometimes) get around this. Most of the listings are limited to 20 or so characters, so I will punch in some random characters, and hit the octothorpe for a new dialtone. That way, the hotel printout merely gets the first, defective, series.

This problem certainly raises some curious questions....

DB
New York City

Why do you think so many phone phreaks work in hotels?

The Facts on 10698

Dear 2600:

On pages 42 and 43 of your wonderful Autumn 1989 issue is a comprehensive list of carrier access codes, and in the third column on page 43 is a footnote, the fourth and fifth sentences of which read as follows: "10698, for example, is used to route local calls via New York Telephone. But since all local calls are routed through New York Telephone anyway, it doesn't really serve much purpose except to occasionally get around PBX restrictions."

The second sentence of the quoted portion above is simply wide of the mark, because you are supposed to use 10698 if you want to route certain interstate inter-LATA calls via New York Telephone instead of via AT&T or another long distance carrier. All local calls — in fact, *all* calls, including local, toll, and long distance calls, which both originate *and* terminate *within* a LATA ("Local Access and Transport Area") — *must* be carried by the local Bell Operating Company (BOC), in accordance with Judge Greene's decree in the antitrust case which resulted in the breakup of the Bell System. Those kinds of calls are often referred to as "intra-LATA calls". Conversely, all calls which originate in one LATA and terminate in another LATA ("inter-LATA calls") *must*, unless the decree carves out an exception, be carried by AT&T or an alternate long distance carrier. As Judge Greene put it in his opinion deciding many of the LATA questions: "Most simply, a LATA marks the boundaries beyond which a Bell Operating Company may not carry telephone calls." That's why the geographic delineation of the LATAs was so important to the BOCs. (Judge Greene's opinion deciding many of the LATA questions may be found beginning at page 990 of volume 569 of "Federal Supplement", which is a series of reports of decisions in the lower Federal courts.)

There are two exceptions to the general inter-LATA call rule which Judge Greene recognized and incorporated into the modified final judgement (the MFJ). Both of the exceptions are in or close to our own backyard (speaking as a resident of Manhattan). Both of the approved modifications recognize and continue a practice which is decades old, and is referred to by Judge Greene in his opinion deciding the question as the "limited corridor exception".

One of the limited corridor exceptions is between five northern counties in New Jersey (Bergen, Essex, Hudson, Passaic, and Union Counties) and New York City (the five boroughs of Manhattan, Bronx, Brooklyn, Queens, and Staten Island). Before the breakup, the New York State portion of the corridor consisted of all the territory in Numbering Plan Areas ("NPAs") 212, 516, and 914, but in his decision, Judge Greene cut the territory down to New York City only (which at that time was NPA 212, but now consists of NPAs 212 and 718). In Judge Greene's words, "The exception would allow New York Telephone and New Jersey Bell to continue their direct switching of traffic and private line demand between New York and New Jersey via Class Five, local trunks, a current 'privileged business' arrangement which would be scaled down from 516 and 914 to New York City only." (Judge Greene's opinion explaining why he decided to make a modification of the final judgement as to the northern corridor appears at page 1018 of volume 569 of "Federal Supplement".)

The other corridor exception is between Philadelphia and its suburbs in Pennsylvania, and Camden

letters, feedback, and information

and its suburbs in New Jersey. In Pennsylvania, the territory comprises five counties: Bucks, Chester, Delaware, Montgomery, and Philadelphia. In New Jersey, there are three counties: Burlington, Camden, and Gloucester. (Judge Greene's opinion explaining why he decided to make another modification of the final judgement as to the southern corridor appears at pages 1019 and 1021-1023 of volume 569 of "Federal Supplement".)

I suppose that in the early days when calls were handled by live operators, the high volume of calls in the two corridors prompted New Jersey Bell to find ways to speed up the calling process by bypassing AT&T Long Lines, and New York Telephone, in the northern corridor, and Bell of Pennsylvania, in the southern corridor, were willing to oblige. (One of your readers who is a real old-timer may be able to give us the correct explanation.) At any rate, this venerable practice has persisted, and was incorporated into the MFJ by Judge Greene.

As a consequence, now if you want to make a northern corridor call from an equal access central office in New Jersey to New York City and bypass AT&T (or whatever long distance company has been chosen), you can do so by first dialing "ten NJB" (10652) and then dialing 1-212 plus the Manhattan or Bronx phone number or 1-718 plus the Brooklyn, Queens, or Staten Island number.

In New York City, if you want to bypass the long distance company and use New York Telephone, you must first dial "ten NYT" (10698) to have the call be listed on the New York Telephone section of your phone bill. New York Telephone hints at how to do this in the white pages, but, surprisingly, doesn't give the 10698 access code.

In Pennsylvania, you must dial "ten BPA" (10272) to make a "Jersey Link" call via Bell of Pennsylvania. To make a "Pennsy-Link" call from New Jersey, you would precede the call with "ten NJB" (10652).

So, the codes 10272, 10652, and 10698 are legitimate access codes, but only for a limited purpose: to make corridor calls via a BOC instead of via a long distance carrier.

The County Man

More Network 2000 Ripoffs

Dear 2600:

I, too, had a similar experience with Network 2000 and the Sprint card last summer in a mall in Nashua, New Hampshire (Winter 89-90, Letters).

The advertising at the Sprint booth mentioned only the FON card, and said nothing about changing long distance carriers. When I asked the woman about getting the FON card, she gave me an application to fill out. But before I signed it, I noticed in the fine print that I was agreeing to change my long distance carrier to Sprint.

I asked the woman if I had read the application right. She at first said no, I was applying for the FON card only. When pressed, however, she finally admitted it, saying, "Well, wouldn't you rather have Sprint?" Only when I declined did she turn the form over, where there was another application for the FON card only.

Needless to say, you know which form was face up on the table, and which form you were told to fill out when you asked for the FON card. It's impossible to tell who the perpetrators were: Network 2000 or their reps.

On another note, ANI in Nashua, NH (and maybe all of 603) was 1-200-222-1111 as of last summer (or maybe it was just 200-222-1111). Oddly enough, it was given to me freely over the phone by a NYNEX tech weenie.

The Iron Warrior
No Fixed Address

Sensitive Material

Dear 2600:

It took close to six weeks to receive my last order of back issues. Do you think customs was pulling some stunts because when I received the parcel it was in a plastic bag and the top of the envelope was ripped and sealed with scotch tape. Is this how you sent them out?

A Dedicated Subscriber

It may take a few weeks to get back issues, but they shouldn't be in a plastic bag or opened in any way. It could have been customs, the post office, or some crazed individual that attacked it somewhere along the line.

Readers: if anything is wrong with your issues, tell us. If there are blank or smudged pages, it's entirely our fault. If your issues are mangled or ripped, it's probably the post office. In that case, tell us AND file a complaint with them.

LISTENING IN

(continued from page 21)

four calling card digits. For the most part radio communications are easy to intercept, and keeping them secure is up to you.

For those of you with scanners who would like to check out marine telephone, here are the frequencies allocated by the FCC. Monitoring marine telephone is a good way to get an inside look at telephone company operations. If you live near the east or west coast, the Mississippi River or the Great Lakes, there will be marine rado activity. During daylight hours you may hear transmissions from hundreds of miles away due to tropospheric ducting propagation.

VHF Marine Radiotelephone Frequencies

Channel	Ship	Shore
24	157.200	161.800
84	157.225	161.825
25	157.250	161.850
85*	157.275	161.875
26	157.300	161.900
86	157.325	161.925
27	157.350	161.950
87	157.375	161.975
28	157.400	162.000
88*	157.425	162.025

* These frequencies are allocated for uses other than marine radiotelephone in certain areas.

INCURSIONS AND INTRUSIONS

(continued from page 7)

ties (and regardless of the possibility that the system is part of the owner's livelihood) is scary to me and should be to anyone responsible for running a system such as this."

Here is a sampling of some of the comments seen around the country after the Jolnet seizure:

→ "As administrator for *Zygot*, should I start reading my users' mail to make sure they aren't saying anything naughty? Should I snoop through all the files to make sure everyone is being good? This whole affair is rather chilling."

→ "From what I have noted with respect to *Jolnet*, there was a serious crime committed there — by the [federal authorities]. If they busted a system with email on it, the Electronic Communication Privacy Act comes into play. Everyone who had email dated less than 180 days old on the system is entitled to sue each of the people involved in the seizure for at least $1,000 plus legal fees and court costs. Unless, of course, the [authorities] did it by the book, and got warrants to interfere with the email of all who had accounts on the systems. If they did, there are strict limits on how long they have to inform the users."

→ "Intimidation, threats, disruption of work and school, 'hit lists', and serious legal charges are *all* part of the tactics being used in this 'witch-hunt'. That ought to indicate that perhaps the use of pseudonyms wasn't such a bad idea after all."

→ "There are civil rights and civil liberties issues here that have yet to be addressed. And they probably won't even be raised so long as everyone acts on the assumption that all hackers are criminals and vandals and need to be squashed, at whatever cost....

"I am disturbed, on principle, at the conduct of at least some of the federal investigations now going on. I know several people who've taken their systems out of public access just because they can't risk the seizure of their equipment (as evidence or for any other reason). If you're a Usenet site, you may receive megabytes of new data every day, but you have no common carrier protection in the event that someone puts illegal information onto the Net and thence into your system."

"The biggest crime that has been committed is that of curiosity."

Increased Restrictions

But despite the outpourings of concern for what had happened, many system administrators and bulletin board operators felt compelled to tighten the control of their systems and to make free speech a little more difficult, for their own protection.

Bill Kuykendall, system administrator for *The Point*, a public UNIX system in Chicago, made the following announcement to the users of his system:

"Today, there is no law or precedent which affords me... the same legal rights that other common carriers have against prosecution should some other party (you) use my property (*The Point*) for illegal activities. That worries me....

"I fully intend to explore the legal questions raised here. In my opinion, the rights to free assembly and free speech would be threatened if the owners of public meeting places were charged with the responsibility of policing all conversations held in the hallways and lavatories of their facilities for references to illegal activities.

"Under such laws, all privately owned meeting places would be forced out of existence, and the right to meet and speak freely would vanish with them. The common sense of this reasoning has not yet been applied to electronic meeting places by the legislature. This issue must be forced, or electronic bulletin boards will cease to exist.

"In the meantime, I intend to continue to operate *The Point* with as little risk to myself as possible. Therefore, I am implementing a few new policies:

"No user will be allowed to post any message, public or private, until his name and address has been adequately verified. Most users in the metropolitan Chicago area have already been validated through the telephone number directory service provided by Illinois Bell. Those of you who received validation notices stating that your information had not been checked due to a lack of time on my part will now have to wait until I get time before being allowed to post.

"Out of state addresses cannot be validated in the manner above.... The short term solution for users outside the Chicago area is to find a system closer to home than *The Point*.

"Some of the planned enhancements to *The Point* are simply not going to happen until the legal issues are resolved. There will be no shell access and no file upload/download facility for now.

"My apologies to all who feel inconvenienced by these policies, but under the circumstances, I think your complaints would be most effective if made to your state and federal legislators. Please do so!"

These restrictions were echoed on other large systems, while a number of smaller hacker bulletin boards disappeared altogether. We've been told by some in the hacker world that this is only a phase, that the hacker boards will be back and that users will once again be able to speak without having their words and identities "registered". But there's also a nagging suspicion, the feeling that something is very different now. A publication has been shut down. Hundreds, if not thousands, of names have been seized from mailing lists and will, no doubt, be investigated. The facts in the 911 story have been twisted and misrepresented beyond recognition, thanks to ignorance and sensationalism. People and organizations that have had contact with any of the suspects are open to investigation themselves. And, around the country, computer operators and users are becoming more paranoid and less willing to allow free speech. In the face of all of this, the belief that democracy will triumph in the end seems hopelessly naive. Yet, it's something we dare not stop believing in. Mere faith in the system, however, is not enough.

We hope that someday we'll be able to laugh at the absurdities of today. But, for now, let's concentrate on the facts and make sure they stay in the forefront.

→ Were there break-ins involving the E911 system? If so, the entire story must be revealed. How did the hackers get in? What did they have access to? What could they have done? What did they actually do? Any security holes that were revealed should already have been closed. If there are more, why do they still exist? Could the original holes have been closed earlier and, if so, why weren't they? Any hacker who caused damage to the system should be held accountable. Period. Almost every hacker around seems to agree with this. So what is the problem? The glaring fact that

"The facts in the 911 story have been twisted and misrepresented beyond recognition, thanks to ignorance and sensationalism."

WELCOME TO THE 90'S

there doesn't appear to have been any actual damage. Just the usual assortment of gaping security holes that never seem to get fixed. Shoddiness in design is something that shouldn't be overlooked in a system as important as E911. Yet that aspect of the case is being side-stepped. Putting the blame on the hackers for finding the flaws is another way of saying the flaws should remain undetected.

> *"Putting the blame on the hackers for finding the flaws is another way of saying the flaws should remain undetected."*

→ Under no circumstance should the *Phrack* newsletter or any of its editors be held as criminals for printing material leaked to them. Every publication of any value has had documents given to them that were not originally intended for public consumption. That's how news stories are made. Shutting down *Phrack* sends a very ominous message to publishers and editors across the nation.

→ Finally, the privacy of computer users must be respected by the government. It's ironic that hackers are portrayed as the ones who break into systems, read private mail, and screw up innocent people. Yet it's the federal authorities who seem to have carte blanche in that department. Just what did the Secret Service do on these computer systems? What did they gain access to? Whose mail did they read? And what allowed them to do this?

Take Exception

It's very easy to throw up your hands and say it's all too much. But the facts indicate to us that we've come face to face with a very critical moment in history. What comes out of this could be a trend-setting precedent, not only for computer users, but for the free press and every citizen of the United States. Complacency at this stage will be most detrimental.

We also realize that one of the quickest ways of losing credibility is to be shrill and conspiracy-minded. We hope we're not coming across in this way because we truly believe there is a significant threat here. If *Phrack* is successfully shut down and its editors sent to prison for writing an article, *2600* could easily be next. And so could scores of other publications whose existence ruffles some feathers. We cannot allow this to happen.

In the past, we've called for people to spread the word on various issues. More times than not, the results have been felt. Never has it been more important than now. To be silent at this stage is to accept a very grim and dark future.

(clip and save)

WHAT MAKES IT ALL WORTHWHILE (COMPLETE AND UNABRIDGED)

"Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances."

the scoop on 911

Documentation on the E911 System
March 1988
$79,449, 6 pages
Bell South Standard Practice
660-225-104SV

Review by Emmanuel Goldstein

It otherwise would have been a quickly forgotten text published in a hacker newsletter. But due to all of the commotion, the Bell South E911 document is now very much in the public eye. Copies are *extremely* easy to come by, despite Bell South's assertion that the whole thing is worth $79,449.

While we can't publish the actual document, we can report on its contents since it's become a news story in itself. But don't get excited. There really isn't all that much here.

Certain acronyms are introduced, among them Public Safety Answering Point (PSAP), also known as Emergency Service Bureau (ESB). This is what you get (in telco lingo) when you dial 911. The importance of close coordination between these agencies is stressed. Selective routing allows the 911 call to be routed to the proper PSAP. The 1A ESS is used as the tandem office for this routing. Certain services made available with E911 include Forced Disconnect, Alternative Routing, Selective Routing, Selective Transfer, Default Routing, Night Service, Automatic Number Identification, and Automatic Location Identification.

We learn of the existence of the E911 Implementation Team, the brave men and women from Network Marketing who help with configuration in the difficult cutover period. This team is in charge of forming an ongoing maintenance subcommittee. We wouldn't want that juicy tidbit to get out, now would we?

We learn that the Switching Control Center (SCC) "is responsible for E911/1AESS translations in tandem central offices". We're not exactly shocked by this revelation.

We also find out what is considered a "priority one" trouble report. Any link down to the PSAP fits this definition. We also learn that when ANI fails, the screens will display all zeroes.

We could go on but we really don't want to bore you. None of this information would allow a hacker to gain access to such a system. All it affords is a chance to understand the administrative functions a little better. We'd like to assume that any outside interference to a 911 system is impossible. Does Bell South know otherwise? In light of their touchiness on the matter, we have to wonder.

We'd be most interested in hearing from people with more technical knowledge on the subject. What does this whole escapade tell us? Please write or call so the facts can be brought forward.

fun and games at a 2600 meeting

In a bizarre story that's still in the process of unfolding, hackers at a 2600 meeting in New York City were monitored by investigative agents of some sort and then harassed by a mob of police.

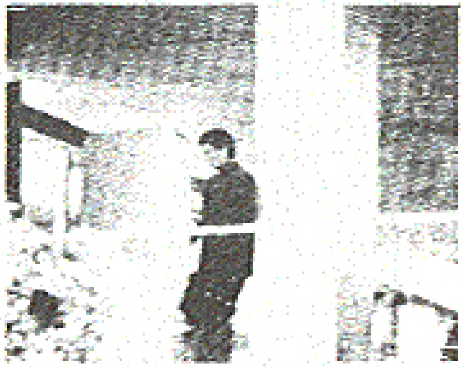
During the meetings, we get quite a few phone calls at the payphones from people all over the world. While one of us was on such a call, the strange man in the suit holding a deskphone was first noticed. Nothing unusual there; Citicorp is filled with suspicious and unusual kinds of people. (We fit right in.) But then we managed to overhear what he was saying. He was describing what the people at the meeting looked like!

Citicorp is just filled with suspicious-looking types.

We started watching him *very* closely. So closely that we're sure he soon realized what a bad undercover investigator he was.

We videotaped him. We took his picture. We recorded his voice. We even tried to be friendly but he got embarrassed and disappeared.

Ten minutes later, close to a dozen cops suddenly materialized on the scene. They demanded to know who we were talking to on the phone. Friends, we told them. Then they told us to hang up.



Who was this strange man?
Why was he watching us?
And what was the deskphone for?

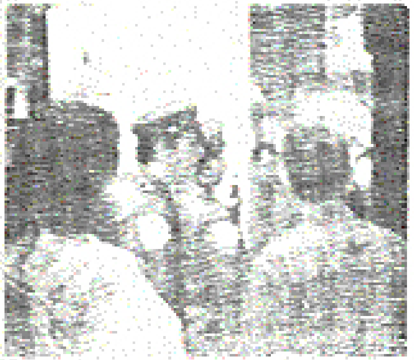
This man found a nice post to lean against for two hours.

"We know you're pranking 911," one of them said to one of us. "Right now we're trying to decide whether or not to lock you up."

Pranking 911? They *had* to be kidding! Maybe a group of five year olds would be doing that, but *not* a group of hackers that knew all about 911 tracing capabilities. More importantly, it was something none of us would ever *want* to do.

We told them this and we asked if they had actually received calls from this location. Did ANI spit out those numbers down at headquarters?

The leader of the cops seemed to get confused at this point and started conferring with some of the others. Then, just as quickly as they had arrived, they left.



Close to a dozen cops suddenly materialized.

The leader of the cops seemed to get confused.

What was it all about? We may never know for sure. But we do know that intimidation tactics and frame-ups will ultimately fail.

Incidentally, 2600 meetings take place in the public lobby of Citicorp in New York City (53rd Street between 3rd and Lexington) from 5 to 8 pm on the first Friday of the month. Those payphone numbers are: 212-223-9011, 212-223-8927, 212-308-8044, 212-308-8162, and 212-308-8184.

There will be several 2600 meetings in California this summer involving American and Dutch hackers. For more information or to meet up with us while we're over there, call 2600 at 516-751-2600.

Relax, it cculd be an innocent tourist taking pictures of all the cops.

Data Network Identification Codes

Most X.25 based public data networks around the world are interconnected using the CCITT X.75 protocol. An addressing scheme for global data networks is the X.121 standard. Under this standard, a host address consists of 14 digits.

```
3110    91400123    01
DNIC    NUA         PORT
```

The above example address is the same as 914123.01 on Telenet. The NUA is the Network User Address of the host machine on that network. The DNIC for Telenet is 3110. The PORT is optional and can be excluded because most host machines will "hunt" from port to port.

A DNIC (Data Network Identification Code) is a 4 digit code that is used to identify the network which will connect you to a host machine. A DNIC is used as a prefix before the NUA (Network User Address). The first digit of the DNIC is one of 7 designated world zones.

Using DNIC's is fairly simple. For example, if I was connected to Telenet and wanted to reach a host on the Austrian DATEX-P network I would use:

```
@ C 2322<NUA>,<NUI>,<PASSWORD>
```

The NUI and PASSWORD are optional if the host machine is willing to accept collect calls. Your NUI and PASSWORD is your account that you have set up with Telenet. It is very similar to a PC Pursuit account. In fact, if you have a PCP account, you can use that to connect to foreign hosts.

The following is a list of DNIC's along with their countries and networks.

Country	DNIC	Network
Antigua	3443	Aganet
Argentina	7220	ARPAC
Argentina	7222	ARPAC
Australia	5052	AUSPAC
Australia	5053	Data Access
Austria	2322	DATEX-P
Austria	2329	RA
Bahamas	3640	BaTelCo
Bahrain	4263	BAHNET
Barbados	3423	
Belgium	2062	DCS
Bermuda	3503	Bermudanet
Brazil	7240	Interdata
Brazil	7241	Renpac
Canada	3020	Datapac
Canada	3025	Globedat
Canada	3028	CNCP
Canada	3106	Tymnet Canada
Cayman Islands	3463	IDAS
Chile	3104	Entel
Chile	7302	Entel
Chile	7303	Chile-PAC
Chile	7305	VTR
China	4600	PTELCOM
Colombia	3107	DAPAQ
Costa Rica	7122	RACSAPAC
Denmark	2382	Datapak
Dominican Rep	3700	UDTS I
Egypt	6020	ARENTO
Finland	2442	Datapak
Fr Antilles	3400	Dompac
Fr Guiana	7420	Dompac
France	2080	Transpac
France	2081	NTI
Gabon	6282	Gabonpac
Germany F.R.	2624	DATEX-P
Greece	2022	Helpak
Greenland	2901	KANUPAX
Guam	5351	PCINET
Guatemala	7043	GAUTEL
Honduras	7080	HONDUTEL
Hong Kong	4542	INTELPAK
Hong Kong	4545	DATAPAK
Hungary	2621	DATEXL
Iceland	2740	Icepak
Indonesia	5101	SKDP
Ireland	2724	Eirpac
Israel	4251	Isranet
Italy	2222	Itapac
Italy	2227	Italcable
Ivory Coast	6122	SYTRANPACI
Jamaica	3380	Jamintel
Japan	4401	NTT DDX
Japan	4406	NISnet
Japan	4408	KDD Venus-P

(continued on page 42)

2600 Marketplace

2600 WILL BE HAVING WEST COAST MEETINGS during the month of July. Hackers from Holland will also be there. Call 516-751-2600 to find out where exactly we'll be or to make suggestions as to where we should go.

VMS HACKERS: For sale: a complete set of DEC VAX/VMS manuals in good condition. Most are for VMS revision 4.2; some for 4.4. Excellent for "exploring"; includes System Manager's Reference, Guide To VAX/VMS System Security, and more. Mail requests to Roger Wallington, P.O. Box 446, Leonia, NJ 07605-0446.

WANTED: Red box plans, kits, etc. Also back issues of Phrack, Syndicate Reports, and any other hack/phreak publications, electronic or print wanted. Send information and prices to Greg B., 2211 O'Hara Dr., Charlotte, NC 28273.

TAP MAGAZINE now has a BBS open for public abuse at 502-499-8933. We also have free issues. You send us a 25 cent stamp and we send you our current issue. Fancy huh? Mail to TAP, P.O. Box 20264, Louisville KY 40250-0264.

SUBSCRIBE TO CYBERTEK, a magazine centered upon technology with topics on computer security. Send $10 for a one year subscription to Cybertek Magazine, PO Box 64, Brewster, NY 10509.

NEEDED: Info on speech encryption (Digicom, Crypto). Send to Hack Tic, P.O. Box 22953, 1100 DL, Amsterdam, The Netherlands.

CYBERPUNKS, HACKERS, PHREAKS, Libertarians, Discordians, Soldiers of Fortune, and Generally Naughty People: Protect your data! Send me a buck and I'll send you an IBM PC floppy with some nifty shareware encryption routines and a copy of my paper "Crossbows to Cryptography: Techno-Thwarting the State." Chuck, The LiberTech Project, 8726 S. Sepulveda Blvd., Suite B-253, Los Angeles, CA 90045.

RARE TEL BACK ISSUE SET (like TAP but strictly telephones). Complete 7 issue 114 page set. $15 ppd. Have photo copy machine self-serve key counter. Would like to trade for red box minus its IC'S. Pete Haas, P.O. Box 702, Kent, Ohio 44240.

WANTED: Red box kits, plans, and assembled units. Also, other unique products. For educational purposes only. Please send information and prices to: TJ, 21 Rosemont Avenue, Johnston, RI 02919.

THE CHESHIRE CATALYST, former editor of the TAP newsletter, has dates available to lecture in Europe in late August and early September. For lecture fees and information on seminars to be given, write to: Richard Cheshire, P.O. Box 641, Cape Canaveral, FL, USA 32920.

KEEP WATCHING this space.

TAP BACK ISSUES, complete set Vol 1-91 of QUALITY copies from originals. Includes schematics and indexes. $100 postpaid. Via UPS or First Class Mail. Copy of 1971 Esquire article "The Secrets of the Little Blue Box" $5 & large SASE w/45 cents of stamps. Pete G., PO Box 463, Mt. Laurel, NJ 08054. We are the Original!

FOR SALE: Manual for stepping switches (c) 1964. This is a true collector's item, with detailed explanations, diagrams, theory, and practical hints. $15 or trade for Applecat Tone Recognition program. FOR SALE: Genuine Bell phone handset. Orange w/tone, pulse, mute, listen-talk, status lights. Fully functional. Box clip and belt clip included. $90 OBO. Please post to S. Foxx, POB 31451, River Station, Rochester, NY 14627.

2600 MEETINGS. First Friday of the month at the Citicorp Center--from 5 to 8 pm in the lobby near the payphones, 153 E 53rd St., NY, between Lex & 3rd. Come by, drop off articles, ask questions. Call 516-751-2600 for more info Payphone numbers at Citicorp: 212-223-9011, 212-223-8927, 212-308-8044, 212-308-8162, 212-308-8184.

Deadline for Summer Marketplace: 7/1/90.

Do you have something to sell? Are you looking for something to buy? Or trade? This is the place! The 2600 Marketplace is free to subscribers! Send your ad to: 2600 Marketplace, P.O. Box 99, Middle Island, NY 11953. Include your address label. Only people please, no businesses.

Data Network Identification Codes (DNIC's) Of The World

(continued from page 40)

Japan	4410	NI+CI
Korea Rep	4501	DACOM-NET
Kuwait	4263	
Lebanon	4155	SODETEL
Luxembourg	2704	Luxpac
Malaysia	5021	Maynet
Mauritius	6170	MauriData
Mexico	3340	TELEPAC
N. Antilles	3620	
N. Marianas	5351	PCInet
Netherlands	2041	Datanet-1
Netherlands	2049	Datanet-1
New Caledonia	5460	Tompac
New Zealand	5301	Pacnet
Norway	2422	Datapak
Panama	7141	
Panama	7142	INTELPAQ
Peru	3104	IMPACS
Philippines	5151	CAPWIRE
Philippines	5152	PGC
Philippines	5154	GMCR
Philippines	5156	ETPI
Polynesia	5470	Tompac
Portugal	2680	Telepac
Portugal	2682	SABD
Puerto Rico	3300	UDTS-I
Puerto Rico	3301	PRTC
Qatar	4271	DOHPAC
Reunion	6470	Dompac
San Marino	2922	X-NET
Saudi Arabia	4263	Bahnet
Singapore	5252	Telepac
South Africa	6550	Saponet
South Africa	6559	Saponet
Spain	2145	Iberpac
Sweden	2402	Datapak
Switzerland	2284	Telepac
Taiwan	4872	PACNET
Taiwan	4877	UDAS
Thailand	5200	IDAR
Tortola, BVI	3483	
Trinidad	3740	Textel
Trinidad	3745	Datanett
Tunisia	6050	RED25
Turkey	2862	Turpac
Turks BWI	3763	
U. Kingdom	2341	BTI IPSS
U. Kingdom	2342	BT PSS
U. Kingdom	2350	Mercury
U. Kingdom	2352	Hull
U.S. Virgin I	3320	UDTS-I
UAE	3104	IMPACS
UAE	4243	EMDAN
Uruguay	7482	
USA	3106	Tymnet
USA	3110	Telenet
USA	3126	Autonet
USA	3134	Accunet
USA	3135	Alascom
USA	3135	Alaskanet
USA	3139	Netexpress
USSR	2502	Iasnet
Zimbabwe	6482	Zimnet

Here is the same list in DNIC order, to help give you a sense of how the codes are allocated.

DNIC	Network	Country
2022	Helpak	Greece
2041	Datanet-1	Netherlands
2049	Datanet-1	Netherlands
2062	DCS	Belgium
2080	Transpac	France
2081	NTI	France
2145	Iberpac	Spain
2222	Itapac	Italy
2227	Italcable	Italy
2284	Telepac	Switzerland
2322	DATEX-P	Austria
2329	RA	Austria
2341	BTI IPSS	U. Kingdom
2342	BT PSS	U. Kingdom
2350	Mercury	U. Kingdom
2352	Hull	U. Kingdom
2382	Datapak	Denmark
2402	Datapak	Sweden
2422	Datapak	Norway
2442	Datapak	Finland
2502	Iasnet	USSR
2621	DATEXL	Hungary
2624	DATEX-P	Germany F.R.
2680	Telepac	Portugal
2682	SABD	Portugal
2704	Luxpac	Luxembourg
2724	Eirpac	Ireland
2740	Icepak	Iceland
2862	Turpac	Turkey
2901	KANUPAX	Greenland
2922	X-NET	San Marino
3020	Datapac	Canada
3025	Globedat	Canada
3028	CNCP	Canada
3104	Entel	Chile
3104	IMPACS	Peru
3104	IMPACS	UAE
3106	Tymnet	USA
3106	Tymnet Canada	Canada
3107	DAPAQ	Colombia
3110	Telenet	USA
3126	Autonet	USA
3134	Accunet	USA
3135	Alascom	USA
3135	Alaskanet	USA
3139	Netexpress	USA
3300	UDTS-I	Puerto Rico
3301	PRTC	Puerto Rico
3320	UDTS-I	U.S. Virgin I
3340	TELEPAC	Mexico
3380	Jamintel	Jamaica
3400	Dompac	Fr Antilles
3423		Barbados
3443	Aganet	Antigua
3463	IDAS	Cayman Islands
3483		Tortola, BVI
3503	Bermudanet	Bermuda
3620		N. Antilles
3640	BaTelCo	Bahamas
3700	UDTS-I	Dominican Rep
3740	Textel	Trinidad
3745	Datanett	Trinidad
3763		Turks BWI
4155	SODETEL	Lebanon
4243	EMDAN	UAE
4251	Isranet	Israel
4263		Kuwait
4263	BAHNET	Bahrain
4263	Bahnet	Saudi Arabia
4271	DOHPAC	Qatar
4401	NTT DDX	Japan
4406	NISnet	Japan
4408	KDD Venus-P	Japan
4410	NI+CI	Japan
4501	DACOM-NET	Korea Rep
4542	INTELPAK	Hong Kong
4545	DATAPAK	Hong Kong
4600	PTELCOM	China
4872	PACNET	Taiwan
4877	UDAS	Taiwan
5021	Maynet	Malaysia
5052	AUSPAC	Australia
5053	Data Access	Australia
5101	SKDP	Indonesia
5151	CAPWIRE	Philippines
5152	PGC	Philippines
5154	GMCR	Philippines
5156	ETPI	Philippines
5200	IDAR	Thailand
5252	Telepac	Singapore
5301	Pacnet	New Zealand
5351	PCINET	Guam
5351	PCInet	N. Marianas
5460	Tompac	New Caledonia
5470	Tompac	Polynesia
6020	ARENTO	Egypt
6050	RED25	Tunisia
6122	SYTRANPACI	Ivory Coast
6170	MauriData	Mauritius
6282	Gabonpac	Gabon
6470	Dompac	Reunion
6482	Zimnet	Zimbabwe
6550	Saponet	South Africa
6559	Saponet	South Africa
7043	GAUTEL	Guatemala
7080	HONDUTEL	Honduras
7122	RACSAPAC	Costa Rica
7141		Panama
7142	INTELPAQ	Panama
7220	ARPAC	Argentina
7222	ARPAC	Argentina
7240	Interdata	Brazil
7241	Renpac	Brazil
7302	Entel	Chile
7303	Chile-PAC	Chile
7305	VTR	Chile
7420	Dompac	Fr Guiana
7482		Uruguay

the 707 area code

by Lunch

The following is a list of all exchanges for area code 707, which runs from the north end of San Francisco Bay to the Oregon border along the wild, windy North Coast of California. This could be useful if you're looking for "hidden" exchanges, ANI, ring back, PacTel test numbers, or just modem tones here in Silicon Valley North.

Pop and org centers are (in no special order) Santa Rosa, Petaluma, Fairfield-Suisun, Eureka, Vacaville, Vallejo, Napa, and Benecia. County codes are: NA (Napa), ME (Mendocino), LA (Lake), SA (Sonoma), MA (Marin), HU (Humboldt), DN (Del Norte), TR (Trinity), and SO (Solano).

224	NA	Napa
226	NA	Napa
247	ME	Piercy
252	NA	Napa
253	NA	Napa
255	NA	Napa
257	NA	Napa
258	NA	Napa
262	LA	Lakeport
270	SA	Santa Rosa
274	LA	Nice
275	LA	Upper Lake
277	LA	Kelseyville
279	LA	Kelseyville
374	SO	Rio Vista
422	SO	Fairfield-Suisun
423	SO	Fairfield-Suisun
424	SO	Fairfield-Suisun
425	SO	Fairfield-Suisun
426	SO	Fairfield-Suisun
427	SO	Fairfield-Suisun
428	SO	Fairfield-Suisun
429	SO	Fairfield-Suisun
431	SA	Healdsburg
433	SA	Healdsburg
437	SO	Fairfield-Suisun
442	HU	Eureka
443	HU	Eureka
444	HU	Eureka
445	HU	Eureka
446	SO	Vacaville
447	SO	Vacaville
448	SO	Vacaville
449	SO	Vacaville
457	DN	Crescent City
458	DN	Crescent City
468	ME	Ukiah
482	DN	Klamath
485	ME	Ukiah
487	DN	Smith River
488	HU	Orick
523	SA	Santa Rosa
525	SA	Santa Rosa
526	SA	Santa Rosa
527	SA	Santa Rosa
528	SA	Santa Rosa
538	SA	Santa Rosa
539	SA	Santa Rosa
542	SA	Santa Rosa
545	SA	Santa Rosa
546	SA	Santa Rosa
552	SO	Vallejo
553	SO	Vallejo
554	SO	Vallejo
557	SO	Vallejo
571	SA	Santa Rosa
573	SA	Santa Rosa
574	TR	Mad River
574	SA	Santa Rosa
575	SA	Santa Rosa
576	SA	Santa Rosa
577	SA	Santa Rosa
578	SA	Santa Rosa
579	SA	Santa Rosa
584	SA	Santa Rosa
585	SA	Santa Rosa
586	SA	Santa Rosa
629	HU	Petrolia
632	SA	Cazadero
642	SO	Vallejo
643	SO	Vallejo
644	SO	Vallejo
645	SO	Vallejo
646	SO	Vallejo
648	SO	Vallejo
664	SA	Petaluma-Rohnert Park
668	HU	Blue Lake
677	HU	Trinidad
722	HU	Pepperwood
725	HU	Fortuna
733	HU	Loleta
743	ME	Potter Valley
744	ME	Hopland
745	SO	Benecia
746	SO	Benecia
747	SO	Benecia
762	SA	Petaluma
763	SA	Petaluma
764	HU	Rio Dell (Scotia)
765	SA	Petaluma
768	HU	Hydesville
777	HU	Bridgeville
778	SA	Petaluma
785	SA	Timber Cove
786	HU	Ferndale
792	SA	Petaluma
794	SA	Petaluma
795	SA	Petaluma
822	HU	Arcata
823	SA	Sebastopol
826	HU	Arcata
829	SA	Sebastopol
833	SA	Kenwood
838	SA	Windsor
839	HU	Arcata
847	SA	Timber Cove
857	SA	Geyserville
864	SO	Fairfield-Suisun
865	SA	Monte Rio
869	SA	Guerneville
874	SA	Occidental
875	SA	Bodega Bay
876	SA	Valley Ford

(continued on page 46)

BOOK REVIEW

The Cuckoo's Egg
By Clifford Stoll
Published by Doubleday
$19.95, 326 pages
ISBN 0-385-24946-2

Review by Dr. Williams

Anybody who's somebody nowadays seems to write a book. Whether it's a celebrity, athlete, or entrepreneur, they all want to tell their story. Clifford Stoll is no exception to this latest craze. In a release by Doubleday, Stoll shares all of his experiences while employed at Berkeley Labs.

In case you might have missed one of Stoll's written articles, TV interviews, or lecture circuit appearances, *The Cuckoo's Egg* is about a year-long effort to apprehend Mark Hess. Hess was a West German hacker breaking into computers all over Europe, North America, and Japan through a tangled web of computer networks. Until his capture, Stoll watched Hess attempt to break into over 400 computer sites on Milnet and Arpanet. Hess was successful in about 40 of his attempts.

Stoll first became aware of the hacker's presence when he discovered a 75 cent accounting error in the Unix system he was administering. One thing led to another, and he realized an unauthorized user was on his system. Instead of getting rid of the account and locking out the hacker, Stoll methodically kept notes and records on the hacker's every move. Stoll alerted all the government agencies that he thought could act upon the case. He started performing traces with the help of Tymnet, a data carrier on which Hess was placing his calls.

As his activities grew, the more interest government agencies showed in Hess. It became apparent the hacker was coming from Europe and showed a strong taste for documents concerning the Star Wars project. The slow wheels of bureaucracy started to move. The FBI, the only agency with the authority to act on the case, officially asked for help from West Germany. With their help, the FBI was able to quickly clamp down on the identity of the hacker. He was arrested nearly one year after Stoll first discovered the accounting error in his system.

The Cuckoo's Egg excels in giving detail into the inner workings of the people involved in capturing Mark Hess. Stoll provides all of the glorious detail of all the agencies involved in the case, what their role was, what their response was to the intrusions, and what their actions were. He tells what the CIA said and did, as well as the NSA and FBI. Everybody's role and their relevance to the case is discussed.

The Cuckoo's Egg provides excellent advice for any network hacker. Stoll explains what traces took place, how long they took to perform, and what the stumbling blocks were in catching the hacker. Stoll tells how many system administrators knew their systems were actually being attacked. If the hacker did succeed in penetrating the system, Stoll describes how many system administrators realized it and what they did once they found out. By seeing the strong and weak spots of system operators and nets, a network hacker is more able to act in a manner which is prudent to his security, while making him aware of more opportunities.

Stoll mentions the techniques used by the hacker to gain access to a system, and the security flaws exploited. The security flaws are not described in detail, but anyone familiar with the computer systems mentioned should already be aware of them.

The Cuckoo's Egg does take Stoll's reactions a bit too far at times. Stoll says the hacker managed to break into an account when all the hacker did was log into a guest account. (Account name: Guest or Anonymous. No password.) He fails to consider that these accounts are set up precisely for guests, regardless of whether or not they log in for malicious reasons.

Stoll also makes too big a deal out of old security holes. He is shocked to learn the Gnu-Emacs holes, which go back to the early 80's (see some of the TAP issues). The X-Preserve hole for the vi editor is another discovery to Stoll, even though that hole is equally well known. Stoll's real shock comes at learning that anybody can take a public readable encrypted password file, and use the same password encryption scheme as the host computer to make dictionary guesses at passwords. This method is perhaps the oldest of them all.

The Cuckoo's Egg also suffers in part from its "novelist" approach at times. Perhaps as a way to stretch out the material, the book is full of irrelevant aspects of Stoll's life and thoughts which have nothing to do with the matter at hand. He constantly bores the reader with personal interactions between him and his wife-to-be, describes how he spent Halloween, Christmas, and every other day, and continually interjects his own "cutesie" observations of life. Stoll also brings back so many immaterial analogies and stories from his grad school days that the reader would think he spent the better part of eight years just to get his master's degree. Most hackers reading the book could hardly give a rip about Stoll's personal life.

From the security standpoint, *The Cuckoo's Egg* stands alone. No other book goes into the gripping detail of the operations used to catch Mark Hess. To Stoll's credit, he kept a detailed lab book of every activity, conversation, and contact during the entire affair. His notes made for an accurate retelling. Any hacker working on a net would benefit from reading this book by learning about the weak spots in the networks as well as how to avoid being tracked down as Mark Hess was.

707 *(continued from page 44)*

877	ME	Elk
878	MA	Tomales
882	ME	Point Arena
884	ME	Gualala
885	SA	Annapolis
887	SA	Forestville
894	SA	Cloverdale
895	ME	Boonville
923	HU	Garberville
925	ME	Leggett
926	HU	Alderpoint
928	LA	Cobb Mountain
935	SA	Sonoma
937	ME	Mendocino
938	SA	Sonoma
942	NA	Calistoga
943	HU	Miranda (Myers Flat)
944	NA	Yountville
946	HU	Weott
961	ME	Fort Bragg
963	NA	St. Helena
964	ME	Fort Bragg
965	NA	St. Helena
966	NA	Lake Berryessa
967	NA	St. Helena
983	ME	Covelo
984	ME	Laytonville
986	HU	Whitethorn
987	LA	Middletown
994	LA	Lower Lake
995	LA	Lower Lake
996	SA	Sonoma
998	LA	Clearlake Oaks

Only ONE exchange in the entire area code that begins with 3? We suspect THAT might be a good place to go hunting.

IT'S EASY

In fact, it's never been easier to renew your subscription to 2600. Just look at your mailing label to find out when your last issue will be. If you have two or fewer issues remaining, it's probably a good idea to renew now and avoid all the heartache that usually goes along with waiting until your subscription has lapsed. (We don't pester you with a lot of reminders like other magazines.) And by renewing for multiple years, you can cheerfully ignore all of the warnings (and occasional price increases) that appear on Page 47.

INDIVIDUAL SUBSCRIPTION

□ 1 year/$18 □ 2 years/$33 □ 3 years/$48

CORPORATE SUBSCRIPTION

□ 1 year/$45 □ 2 years/$85 □ 3 years/$125

OVERSEAS SUBSCRIPTION

□ 1 year, individual/$30 □ 1 year, corporate/$65

LIFETIME SUBSCRIPTION

□ $260 (you'll never have to deal with this again)

BACK ISSUES (never out of date)

□ 1984/$25 □ 1985/$25 □ 1986/$25 □ 1987/$25
□ 1988/$25 □ 1989/$25

(OVERSEAS: ADD $5 PER YEAR OF BACK ISSUES)

TOTAL AMOUNT ENCLOSED: □